Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Σχεδιασμός και Υλοποίηση Εκπαιδευτικής Δραστηριότητας για Αντιμετώπιση της Κοινωνικής Μηχανικής

Απόστολος Χαραλάμπους

Επιβλέπων Καθηγήτρια
Δρ. Ιλιάνα Σταύρου

Μάϊος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Σχεδιασμός και Υλοποίηση Εκπαιδευτικής Δραστηριότητας για Αντιμετώπιση της Κοινωνικής Μηχανικής

Απόστολος Χαραλάμπους

Επιβλέπων Καθηγητής
Δρ. Ιλιάνα Σταύρου

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάϊος 2023

Περίληψη

Ως Κοινωνική Μηχανική περιγράφεται η διαδικασία κατά την οποία αποσπώνται πληροφορίες από ανυποψίαστα άτομα με τη χρήση διαφόρων μεθόδων και μέσων. Στις μέρες μας παράλληλα με την ανάπτυξη της τεχνολογίας, παρατηρείται ραγδαία αύξηση των επιθέσεων Κοινωνικής Μηχανικής με αποτέλεσμα τα ποσοστά των πολιτών και οργανισμών που γίνονται θύματα επιθέσεων να αυξάνονται καθημερινώς.

Ο κύριος στόχος αυτής της μεταπτυχιακής διατριβής, είναι η υλοποίηση εκπαιδευτικής δραστηριότητας, με σκοπό την αναγνώριση επιθέσεων και των κακών πρακτικών της Κοινωνικής Μηχανικής. Παράλληλα, οι συμμετέχοντες μπορούν να ενημερωθούν για τις καλές πρακτικές που έχουν στη διάθεση τους, καθώς επίσης και τον τρόπο με τον οποίο μπορούν να τις εφαρμόζουν.

Μέσα από έρευνα που διεξήχθη, έχουν εντοπιστεί οι σημαντικότερες και συχνότερες μορφές επιθέσεων Κοινωνικής Μηχανικής που χρησιμοποιούνται τα τελευταία χρόνια εις βάρος πολιτών και οργανισμών. Βάση των αποτελεσμάτων της έρευνας, σχεδιάστηκε και υλοποιήθηκε η εκπαιδευτική δραστηριότητα η οποία αποτελείται από 8 σενάρια όπου ο συμμετέχοντας καλείται να επιλέξει την ορθή απάντηση μέσα από τις 3 επιλογές που έχει στη διάθεση του σε κάθε ένα από αυτά. Σε κάθε λάθος απάντηση, υποδεικνύεται στον συμμετέχοντα ο λόγος για τον οποίο η συγκεκριμένη επιλογή θεωρείται λανθασμένη και έπειτα είτε προβάλλεται βίντεο μικρής διάρκειας, είτε εικόνα που συνοδεύεται από ενημερωτικό κείμενο, με σκοπό την ενημέρωση του για τη συγκεκριμένη επίθεση.

Στη συνέχεια, γίνεται αξιολόγηση της εκπαιδευτικής δραστηριότητας, από άτομα τα οποία κατέχουν εμπειρία σε θέματα ασφάλειας υπολογιστών, ασφάλειας δικτύων καθώς επίσης και προστασίας δεδομένων, έτσι ώστε να εκτιμηθεί η καταλληλόλητα του περιεχομένου και να διαπιστωθεί σε τι βαθμό επιτυγχάνονται οι στόχοι της δραστηριότητας.

Ως εκ τούτου, η εκπαιδευτική δραστηριότητα συνοδεύεται από ερωτηματολόγιο, στο οποίο καλούνται οι συμμετέχοντες να απαντήσουν. Από το ερωτηματολόγιο γίνεται λήψη και ανάλυση των αποτελεσμάτων, μέσα από τα οποία παρουσιάζεται η αποτελεσματικότητα της δραστηριότητας και ο βαθμός στον οποίο μπορεί να θεωρηθεί σημαντική ως μέτρο αντιμετώπισης των επιθέσεων Κοινωνικής Μηχανικής.

Summary

Social Engineering describes the process in which information is extracted from unsuspecting people using various methods and means. Nowadays, along with the development of technology, there is also a rapid increase in Social Engineering attacks, which leads to daily increase the number of citizens and organizations that become victims of social engineering attacks.

The main objective of this master's thesis is the implementation of an educational activity, regarding the identification of attacks and bad practices of Social Engineering. At the same time, participants can be informed about the good practices and the way they can use them.

From the literature review, has been identified the most important and frequent attacks of Social Engineering used in recent years. Based on those results, the educational activity was designed and developed. It consists of 8 scenarios where the participant has to choose the correct answer from 3 available options. When a participant chooses a wrong answer, the activity represents to the participant the reason why that choice is considered incorrect, and then a short video or image accompanied by informative text presented giving information about the particular attack method.

The educational activity is evaluated by people who have experience in computer security, network security and data protection, in order to evaluate the appropriateness of the content and to determine whether the objectives of the activity are achieved.

Therefore, the educational activity is accompanied by a questionnaire which must be completed by the participants. When the questionnaire is completed, the results are received and analyzed. Thought the results, will be presented the effectiveness of the activity and the extent to which it can be considered relevant as a countermeasure against social engineering attacks.

Ευχαριστίες

Η ολοκλήρωση της μεταπτυχιακής διατριβής , θα ήταν αδύνατη χωρίς τη πολύτιμη υποστήριξη και καθοδήγηση της καθηγήτριας μου Δρ. Ιλιάνας Σταύρου, του Ανοικτού Πανεπιστημίου Κύπρου. Της εκφράζω ένα μεγάλο ευχαριστώ για όλη τη βοήθεια που μου προσέφερε κατά τη διάρκεια αυτή.

Θέλω επίσης να ευχαριστήσω τη σύζυγο μου Πατρίτσια Κυριάκου για την αμέτρητη συμπαράσταση, κατανόηση επιμονή και υπομονή που έδειξε καθ' όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου, οι οποίοι πάντοτε υπήρξαν ένα ανεκτίμητο στήριγμα για εμένα και στους οποίους οφείλω όλη τη διαδρομή των σπουδών μου μέχρι σήμερα.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Στις μέρες μας, οι ενέργειες μέσω διαδικτύου και η επαφή με τον κυβερνοχώρο είναι δεδομένη και απαραίτητη. Σε ολόκληρο τον επιχειρηματικό κόσμο παρατηρείται μια στροφή προς τη χρήση του ηλεκτρονικού εμπορίου, την εξ αποστάσεως εξυπηρέτηση και την ραγδαία εξάρτηση από τις ηλεκτρονικές υπηρεσίες. Μέσα σε όλη αυτήν την ηλεκτρονική δραστηριότητα, γίνεται και η αναγκαστική χρήση δεδομένων και πληροφοριών προσωπικού χαρακτήρα.

Η ασφάλεια των δεδομένων, αποτελεί μείζον ζήτημα που επηρεάζει όλους τους τομείς χωρίς κάποια εξαίρεση και αφορά την προστασία των πληροφοριών και συστημάτων από μη εξουσιοδοτημένη χρήση, πρόσβαση, τροποποίηση, αφαίρεση, παραβίαση ή κλοπή.

Προσωπικά στοιχεία και ευαίσθητες πληροφορίες όπως όνομα χρήστη, κωδικός πρόσβασης, αριθμός πιστωτικής κάρτας, στοιχεία λογαριασμού, είναι μερικά από τα δεδομένα τα οποία χρησιμοποιούνται καθημερινώς είτε μέσω διαδικτύου είτε δια ζώσης, και αποτελούν στόχο για τους εγκληματίες του κυβερνοχώρου. [01]

Παρόλο που γίνεται προσπάθεια από την πολιτεία για θέσπιση νόμων με σκοπό την προστασία των χρηστών από διαρροές προσωπικών δεδομένων καθώς και νόμων για να εξασφαλιστεί το απόρρητό τους όταν είναι αναγκαία η δημοσιοποίησή τους, εντούτοις παρατηρείται ότι ο στόχος αυτός δεν επιτυγχάνεται. [02]

Η Κοινωνική Μηχανική (Social Engineering), φαίνεται να αποτελεί την πιο συχνή μορφή κυβερνοαπειλής που καλείται να αντιμετωπίσει ο πλανήτης στις μέρες μας. Οι επιθέσεις Κοινωνικής Μηχανικής, έχουν αυξηθεί ραγδαία τόσο μέσω διαδικτύου όσο και δια ζώσης, με αποτέλεσμα την αποδυνάμωση της κυβερνοασφάλειας αλλά και την αύξηση του αριθμού των πολιτών που δέχονται αυτού του είδους επιθέσεις.

1.1 Πρόβλημα Κοινωνικής Μηχανικής

Με τον όρο Κοινωνική Μηχανική, θεωρούμε τον κάθε δυνατό τρόπο και μέσο με το οποίο ένας επιτιθέμενος μπορεί να αποσπάσει προσωπικές πληροφορίες και στοιχεία από ένα άτομο ή μια επιχείρηση, ως προς το συμφέρων των εγκληματιών του κυβερνοχώρου. [03] Αυτό, μπορεί να επιτευχθεί μέσα από διάφορες κακόβουλες δραστηριότητες οι οποίες μπορούν να αποπλανήσουν ή να επηρεάσουν ψυχολογικά ένα άτομο με απώτερο σκοπό την αποκάλυψη εμπιστευτικών πληροφοριών είτε την παραβίαση μέτρων ασφαλείας. [04]

Υψηλά στο στόχο των επιτιθέμενων εκτός από απλοί πολίτες, βρίσκονται μεγάλες επιχειρήσεις, γνωστά άτομα, τράπεζες και οργανισμοί ενός κράτους. Ο κίνδυνος ύπαρξης ενός τέτοιου είδους επίθεσης, αυξάνεται στις μέρες μας, όπου διάφοροι αναζητούν ευκαιρίες έτσι ώστε μέσα από ενέργειες, να κερδίσουν κάποιο όφελος είτε είναι οικονομικό, πολιτικό και κοινωνικό είτε να προκαλέσουν ζημιά για θέματα ανταγωνισμού.

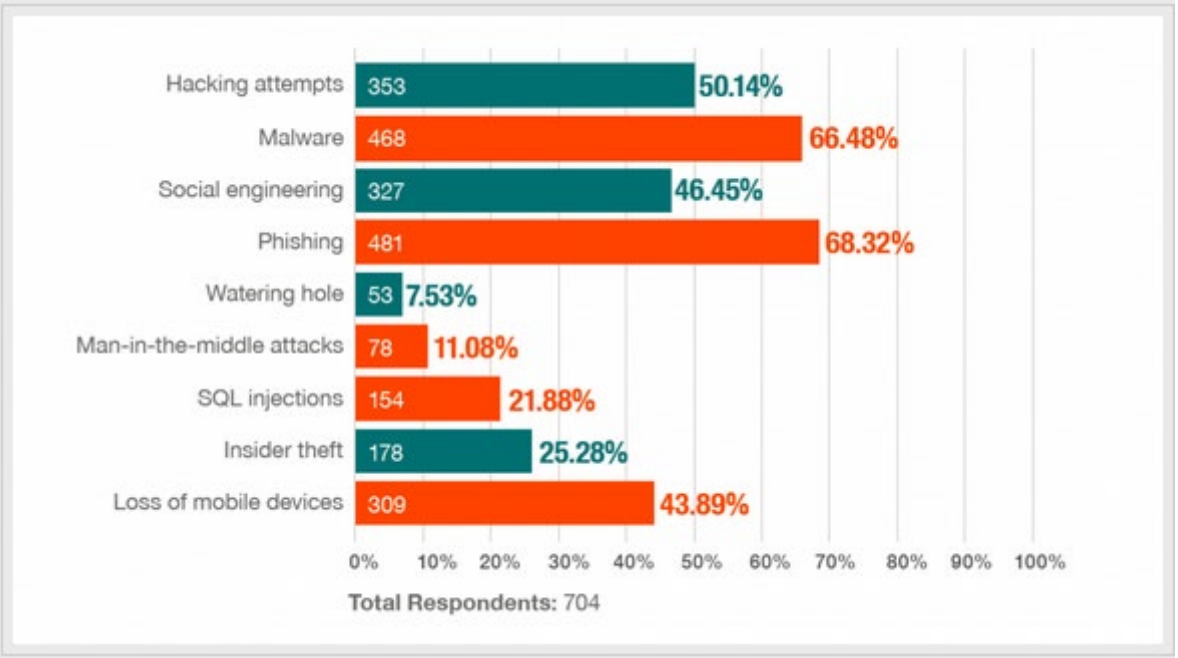
Στόχος των επιτιθέμενων, είναι η συλλογή προσωπικών πληροφοριών όπως για παράδειγμα κωδικοί πρόσβασης, ονόματα χρηστών κ.α., τα οποία στη συνέχεια θα χρησιμοποιηθούν ως μέσω εκβίασης, απειλής, ή και χρήσης τους με σκοπό την απόσπαση χρημάτων είτε την πρόκληση κακόβουλης ζημιάς.

1.2 Στατιστικά στοιχεία

Μέσα από στοιχεία που παρέχονται από διάφορες εταιρείες και οργανισμούς, παρουσιάζεται το πρόβλημα της Κοινωνικής Μηχανικής, η ραγδαία αύξηση του τα τελευταία χρόνια καθώς επίσης και οι συχνότερες μέθοδοι που επιλέγουν οι επιτιθέμενοι να χρησιμοποιήσουν.

Αποτελέσματα του οργανισμού ISACA δείχνουν ότι επιθέσεις ψαρέματος (Phishing Attacks) καθώς επίσης και άλλα είδη επιθέσεων Κοινωνικής Μηχανικής ήταν οι πιο συχνές μορφές επιθέσεων σε επιχειρήσεις για το έτος 2014, με ποσοστό σχεδόν το 70%. Αυτού του τύπου επιθέσεις είχαν ως αποτέλεσμα κάποιας εκμετάλλευσης στην επιχείρηση. Αντίστοιχα, ποσοστό ίσο με 50% αντιστοιχεί σε διάφορα άλλα είδη επιθέσεων Κοινωνικής Μηχανικής, όπως είναι water-holing attacks, SMS phishing (SmiShing) και Voice Phishing (Vishing).[05]

Τα στοιχεία αυτά, παρουσιάζονται στην γραφική παράσταση που ακολουθεί, όπου διακρίνονται και άλλοι τύποι επιθέσεων όπως είναι Malware attacks με ένα υψηλό ποσοστό της τάξεως του 66,68%, SQL Ingestions με ποσοστό 21,88% και Man in the middle attacks με ποσοστό 11,08%. [05]



Εικόνα 1.1: Τύποι επιθέσεων και Ποσοστά [05]

Κατά το έτος 2017, φαίνεται ότι το πρόβλημα συνεχίζει να υπάρχει και μάλιστα να έχει αυξηθεί δραματικά. Αυτό διαπιστώνεται μέσα από στατιστικά στοιχεία που δίνει στη δημοσιότητα η εταιρεία 'Global Sign', στα οποία αναφέρεται ότι 978 εκατομμύρια άνθρωποι σε 20 χώρες έχουν δεχθεί επιθέσεις Κοινωνικής Μηχανικής. Αντίστοιχα, η ιστοσελίδα 'Web Tribunal' παρέχει πληροφορίες για το έτος 2020 στις οποίες αναφέρει ότι μία επίθεση ransomware είναι επιτυχής κάθε 11 δευτερόλεπτα και ποσοστό της τάξης του 75% των εταιριών παγκόσμιος έπεσαν θύματα επιθέσεων τύπου phishing. [06] Στις μέρες μας σε πρόσφατη ενημέρωση για το έτος 2022, η εταιρεία Purplesec αποκάλυψε ότι οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν επιθέσεις Κοινωνικής Μηχανικής σε ποσοστό 98% έναντι άλλων τύπων επιθέσεων.

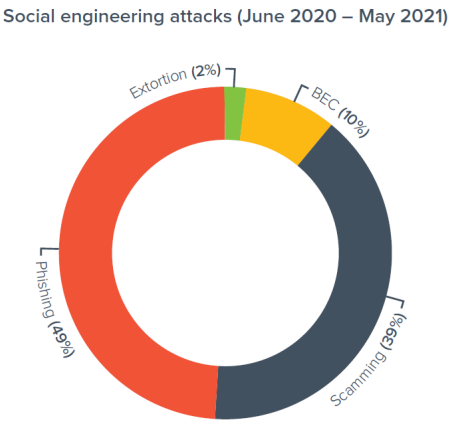
Τα τελευταία χρόνια, ένα μεγάλο πρόβλημα που αντιμετωπίζει ο πλανήτης είναι η πανδημία κορωνοϊού, η οποία, μεταξύ άλλων, επέφερε πολλές αλλαγές στον τρόπο ζωής των ανθρώπων. Αρκετοί οργανισμοί, καθιέρωσαν την εξ αποστάσεως εργασία και έτσι δόθηκε η ευκαιρία σε εγκληματίες του κυβερνοχώρου, να εκμεταλλευτούν αυτό το γεγονός με σκοπό να δελεάσουν

τους χρήστες του διαδικτύου για να υποπέσουν σε επιθέσεις Κοινωνικής Μηχανικής, επιχειρώντας διάφορους τρόπους επιθέσεων και κυρίως επιθέσεις ψαρέματος (phishing attacks).

Σύμφωνα με τα στοιχεία του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ), οι εγκληματίες εκμεταλλεύονται την πανδημία με την αποστολή κακόβουλων ηλεκτρονικών μηνυμάτων, λογισμικών και εφαρμογών. Μέσα από αυτά, ισχυρίζονται ότι προέρχονται από τον ΠΟΥ ή σε άλλους οργανισμούς δημόσιας υγείας και ότι το περιεχόμενο τους αναφέρεται σε συμβουλές και πληροφορίες για τον κορωνοϊό.[07] Στόχος είναι τα θύματα να χρησιμοποιήσουν τον σύνδεσμο ή την εφαρμογή, τα οποία θα τους παραπέμψουν σε μια κακόβουλη ιστοσελίδα όπου θα εισάγουν προσωπικά τους δεδομένα.

Η εταιρεία Barracuda Networks, η οποία παρέχει υπηρεσίες ασφάλειας, παράδοσης εφαρμογών και προστασίας δεδομένων, δημοσίευσε έκθεση με στοιχεία από διάφορους τρόπους επίθεσης, μέσα από την οποία διαπιστώνεται το μεγάλο πρόβλημα που συνεχίζει να υπάρχει. [08]

Τη μεγαλύτερη έξαρση σε διάστημα ενός έτους (από τον Ιούνιου 2020 μέχρι τον Μάιο 2021) κατά τη διάρκεια της πανδημίας φαίνεται ότι είχαν οι επιθέσεις Κοινωνικής Μηχανικής και συγκεκριμένα το Phishing, Scamming, BEC και Extraction. Συγκεκριμένα, το μεγαλύτερο ποσοστό, κατέγραψαν οι επιθέσεις τύπου Phishing με ποσοστό 49%, και ακολούθως οι επιθέσεις τύπου Scamming με ποσοστό 39%. Στη συνέχεια ακολουθούν τύποι επιθέσεων με μικρότερα ποσοστά και αναφέρονται στις επιθέσεις BEC και Extraction οι οποίες αποτελούν το 10% και 2% αντίστοιχα. Τα στοιχεία αυτά παρουσιάζονται στην εικόνα που ακολουθεί.[08]

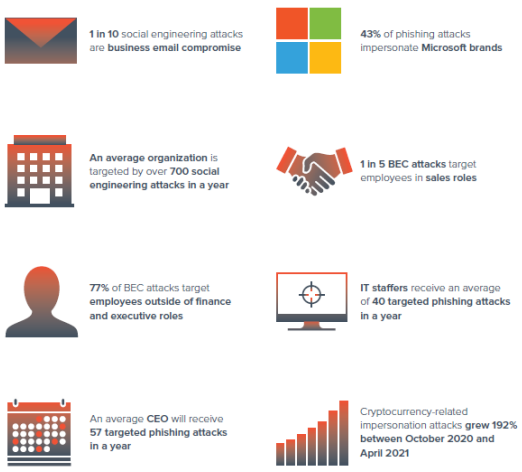


Εικόνα 1.2: Επιθέσεις Κοινωνικής Μηχανικής Ιούνιος 2020 –Μάιος 2021 [08]

Επιπρόσθετα, η ίδια εταιρεία, συγκέντρωσε και παρουσίασε στοιχεία αναφορικά με τους διάφορους τρόπους επιθέσεων Κοινωνικής Μηχανικής. Συγκεκριμένα, οι ακόλουθες πληροφορίες χρησιμοποιούνται με σκοπό να αναδείξουν τη σοβαρότητα του προβλήματος.

- Ένας μεσαίος οργανισμός γίνεται στόχος επιθέσεων Κοινωνικής Μηχανικής περισσότερο από 700 φορές το χρόνο
- Μια στις 5 επιθέσεις BEC, στοχεύουν σε υπαλλήλους με καθήκοντα πωλητή
- Ένας CEO ενός οργανισμού, θα λάβει 57 επιθέσεις τύπου ψαρέματος κατά τη διάρκεια ενός έτους
- Το 43% των επιθέσεων ψαρέματος υποδύονται ότι έχουν ως εμπορική επωνυμία τη Microsoft
- Το 77% των επιθέσεων τύπου BEC, έχουν ως στόχο υπαλλήλους οι οποίοι είναι εκτός χρηματοοικονομικών θεμάτων
- Τα τμήματα IT λαμβάνουν μέσο όρο 40 μηνύματα κάθε χρόνο τα οποία στοχεύουν σε επιθέσεις ψαρέματος
- Οι επιθέσεις πλαστοπροσωπίας που σχετίζονται με κρυπτονομίσματα αυξήθηκαν μέχρι 192% κατά την περίοδο μεταξύ Οκτώβρη 2020 και Απρίλιο 2021. [08]

Οι πληροφορίες αυτές, διακρίνονται στην εικόνα 1.3, όπως έχουν παρουσιαστεί από την εταιρεία.



Εικόνα 1.3: Τύποι επιθέσεων Κοινωνικής Μηχανικής [08]

1.3 Ενημερωτικές Δράσεις και Αποτελεσματικότητα

Σημαντικός παράγοντας ο οποίος θεωρείται απαραίτητος για την αντιμετώπιση επιθέσεων Κοινωνικής Μηχανικής, είναι η επίγνωση του κινδύνου που μπορεί να επιφέρει μια επίθεση και η αντίληψη της ζημιάς που πιθανόν να προκληθεί σε ένα άτομο ή οργανισμό.

Οι τρόποι αντιμετώπισης της Κοινωνικής Μηχανικής, βασίζονται σε 3 βασικά στοιχεία: [09]

1. Την εκπαίδευση και ενημέρωση προσωπικού και πολιτών
2. Την πρακτική έρευνα σε θέματα τρωτότητας ενός οργανισμού
3. Στους εσωτερικούς κινδύνους καθώς επίσης και στη δημιουργία πολιτικών και διαδικασιών ασφαλείας και διαχείρισης μιας πληροφορίας. [09]

Η εκπαίδευση και ενημέρωση σε θέματα Κοινωνικής Μηχανικής, θεωρείται απαραίτητη και έχει ως σκοπό τη δημιουργία μιας κουλτούρας σε θέματα κυβερνοασφάλειας με την έννοια των αντιλήψεων, πεποιθήσεων και συμπεριφορών που συμβάλλουν στην προστασία σημαντικών και ευαίσθητων πληροφοριών. Παράλληλα, η έρευνα σε θέματα τρωτότητας σε έναν οργανισμό, θεωρείται ο έλεγχος που γίνεται για τον εντοπισμό κενών και ευπαθειών στο σύστημα, στο δίκτυο ή ακόμη και στο κτήριο ενός οργανισμού. Αυτά μπορεί να εκμεταλλευθούν από έναν επιτιθέμενο για να αποκτήσει πρόσβαση προβαίνοντας έτσι σε διάφορες ενέργειες που αφορούν τη συλλογή πληροφοριών, την ανάγνωση αρχείων, την αλλαγή και διαγραφή δεδομένων και την εγκατάσταση κακόβουλου λογισμικού. [09]

Επαγγελματίες και οργανισμοί κυβερνοασφάλειας πληροφοριών, επιχειρούν να ενημερώσουν τους πολίτες και τους οργανισμούς για τους κινδύνους που διατρέχουν από επιθέσεις Κοινωνικής Μηχανικής. Οι ενημερώσεις, γίνονται είτε με τη χρήση ενημερωτικού υλικού το οποίο παρέχεται στη διάθεση των πολιτών μέσα από έντυπα, από αναρτήσεις στο διαδίκτυο, από αναφορές που γίνονται στα Μέσα Μαζικής Ενημέρωσης (ΜΜΕ) για τις επιθέσεις της Κοινωνικής Μηχανικής καθώς επίσης και μέσα από διάφορα σεμινάρια τα οποία παρέχονται.

Αυτού του είδους εκπαιδεύσεις και ενημερώσεις που γίνονται από πλευρά οργανισμών και ειδικών συχνά έχουν παθητικό χαρακτήρα, χωρίς να προσελκύσουν κάποιο ενδιαφέρον και ως εκ τούτου να μην επιφέρουν τα επιθυμητά αποτελέσματα. Όπως διαπιστώνεται, δεν επαρκούν για

να μεταφέρουν τη γνώση και την κατανόηση των καλών πρακτικών που χρειάζεται να χρησιμοποιούνται, καθώς οι προσπάθειες που γίνονται με στόχο την αντιμετώπιση των απειλών Κοινωνικής Μηχανικής να αποδεικνύονται ανεπιτυχείς εφόσον πολίτες και οργανισμοί συνεχίζουν να είναι θύματα επιθέσεων.

1.4 Αποτελεσματική αντιμετώπιση του προβλήματος

Συλλέγοντας στοιχεία αναφορικά με τις επιθέσεις Κοινωνικής Μηχανικής και στη συνέχεια προβαίνοντας στην ανάλυση τους, διαπιστώνονται τα προβλήματα που υπάρχουν και συμπεραίνεται ότι για την αποτελεσματική αντιμετώπιση των επιθέσεων Κοινωνικής Μηχανικής, απαιτείται συνεχής ενημέρωση και εκπαίδευση των πολιτών. Σκοπός της αντιμετώπισης είναι η μείωση των επιτυχημένων επιθέσεων και η αποτροπή όσο το δυνατόν περισσότερο από αυτών.

Η διαδραστικότητα, η δυνατότητα δηλαδή για αμφίδρομη επικοινωνία, είναι αυτή που απουσιάζει από τις προσπάθειες ενημέρωσης και από τους τρόπους αντιμετώπισης του προβλήματος της Κοινωνικής Μηχανικής. Το κενό αυτό μπορεί να συμπληρωθεί με τη χρήση εκπαιδευτικής δραστηριότητας, προωθώντας με τον τρόπο αυτό την ενημέρωση και την εκμάθηση για τους κινδύνους της Κοινωνικής Μηχανικής. [10]

Στόχος της δραστηριότητας, είναι να αφυπνίσει στους χρήστες το αίσθημα κινδύνου έναντι των επιθέσεων, να γίνει ανασκόπηση στις κυριότερες και συχνότερες επιθέσεις Κοινωνικής Μηχανικής, να αναδείξει τους τρόπους με τους οποίους γίνεται χρήση των επιθέσεων και παράλληλα, να ενημερώσει τους χρήστες για τους τρόπους αντιμετώπισης κάθε τύπου επίθεσης.

Αναλυτικότερα, μέσα από τη δραστηριότητα, θα παρουσιάζονται οι διάφορες μέθοδοι και τεχνικές που χρησιμοποιούνται κατά τις επιθέσεις Κοινωνικής Μηχανικής με τρόπο που να γίνεται αντιληπτό ότι το κάθε άτομο να έχει τη δυνατότητα ανά πάσα στιγμή και χωρίς να το αντιληφθεί να γίνει θύμα κοινωνικής επίθεσης. Επιπρόσθετα, θα δίνει το μήνυμα ότι τόσο η διαφύλαξη όσο και η απόκρυψη στοιχείων και προσωπικών δεδομένων θεωρείται απαραίτητη και εξίσου σημαντική. Παράλληλα, εφόσον έχουμε να αντιμετωπίσουμε διάφορα είδη επιθέσεων, θα έχει ως στόχο να παρουσιάσει στους χρήστες τα μέτρα αντιμετώπισης έναντι των κυριότερων επιθέσεων και ταυτόχρονα, να γίνεται παρουσίαση στοιχείων που μπορούν να χρησιμοποιηθούν έτσι ώστε ο χρήστης να αντιλαμβάνεται ότι πιθανόν να γίνεται προσπάθεια εξαπάτησης του μέσω επιθέσεων Κοινωνικής Μηχανικής.

Παρόλα αυτά, θεωρείται δεδομένο ότι ακόμα και με αυτό τον τρόπο ενημέρωσης, τόσο οι οργανισμοί όσο και πολίτες, δεν πρέπει να καθησυχάζονται και να θεωρούν ότι είναι πλήρως ασφαλείς από αυτού του είδους επιθέσεις. Καθώς η τεχνολογία εξελίσσεται και συνεχώς νέοι τρόποι επιθέσεων δημιουργούνται, απαιτείται η ενημέρωση να είναι συστηματική, συνεχής, να γίνεται ανά τακτά χρονικά διαστήματα και να ανανεώνεται με βάση τα νέα δεδομένα που δημιουργούνται [09]. Το αίσθημα της ανασφάλειας θα υπάρχει, σε μειωμένο όμως βαθμό, καθώς η τεχνολογία εξελίσσεται και συνεχώς νέοι τρόποι επιθέσεων εμφανίζονται.

Κεφάλαιο 2

Βιβλιογραφική Ανασκόπηση

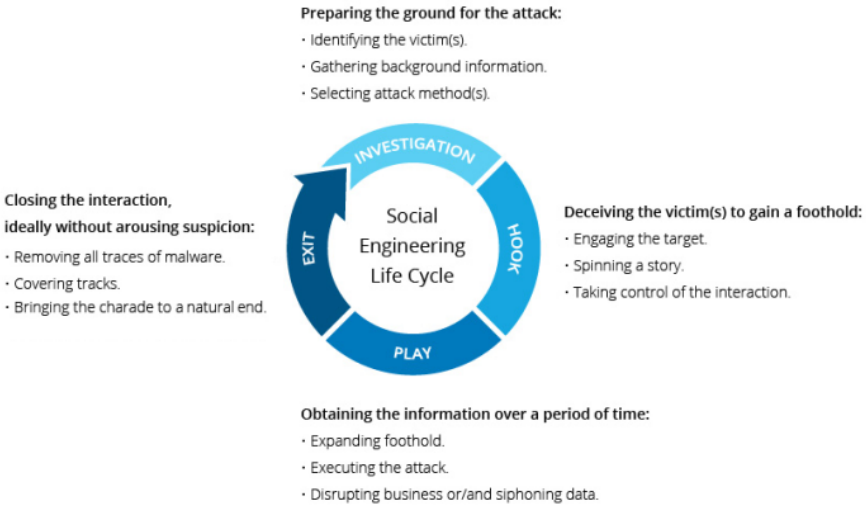
2.1 Ανάλυση επιθέσεων Κοινωνικής Μηχανικής

Οι επιθέσεις Κοινωνικής Μηχανικής μπορεί να γίνουν σε ένα ή περισσότερα βήματα και δεν απαιτούν εξελιγμένη γνώση της κυβερνοασφάλειας. Αν και οι επιθέσεις Κοινωνικής Μηχανικής διαφέρουν μεταξύ τους, έχουν ένα κοινό μοτίβο με παρόμοιες φάσεις το οποίο μπορεί να παρουσιαστεί ως ο Κύκλος Ζωής της Κοινωνικής Μηχανικής. Ο κύκλος αυτός παρουσιάζει τις διαδικασίες και τα στάδια που αποτελείται μια επίθεση, αρχίζοντας από την έρευνα, προχωρώντας στην εξαπάτηση του θύματος, στη συνέχεια εκτελείται η επίθεση και ως τελευταίο βήμα είναι το κλείσιμο της επίθεσης.

Αναλυτικότερα, κατά την εκτέλεση του Κύκλου Ζωής της Κοινωνική Μηχανικής, ακολουθείται η πιο κάτω διαδικασία, τα οποία παρουσιάζονται στην Εικόνα 2.1:

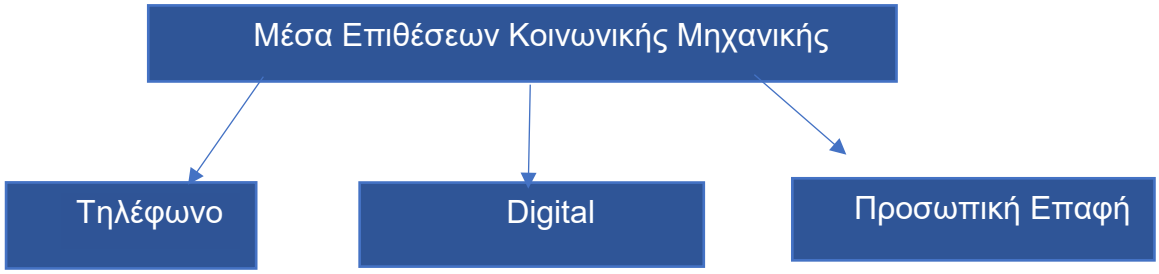
- Έρευνα → Είναι το αρχικό βήμα σε μια επίθεση Κοινωνικής Μηχανικής κατά την οποία επιλέγεται το θύμα με βάση ορισμένες απαιτήσεις. Θεωρείται η διαδικασία κατά την οποία γίνεται η ταυτοποίηση του θύματος, η συλλογή πληροφοριών για το θύμα καθώς επίσης και την επιλογή του τρόπου επίθεσης που θα εκτελεστεί.
- Συλλογή → Στη δεύτερη φάση του κύκλου ζωής βρίσκεται η διαδικασία συλλογής δεδομένων και στοιχείων. Διαδικασία κατά την οποία ο επιτιθέμενος αρχίζει να κερδίζει την εμπιστοσύνη του θύματος και στη συνέχεια να γίνεται η αλληλεπίδραση και εξαπάτηση του θύματος είτε με προσωπική επαφή είτε εξ αποστάσεως.
- Εκτέλεση → Κατά τη τρίτη φάση γίνεται η εκτέλεση της επίθεσης. Διαδικασία κατά την οποία ο επιτιθέμενος αρχικά επηρεάζει το θύμα προκειμένου να παρέχει ευαίσθητες πληροφορίες ή να υποστεί σε κάποιο λάθος ασφαλείας. Ακολούθως, εκτελείται η επίθεση και συλλέγονται οι πληροφορίες του θύματος.
- Έξοδος → Είναι το τελευταίο βήμα στο οποίο γίνεται μετά την επιτυχημένη επίθεση. Κατά τη διαδικασία αυτή, γίνεται αφαίρεση όλων των μέσων που έχουν χρησιμοποιηθεί, καθώς

επίσης και την απόκρυψη για όλα τα στοιχεία κακόβουλου λογισμικού καλύπτοντας έτσι τυχόν ίχνη. [11]



Εικόνα 2.1: Κύκλος Ζωής Κοινωνικής Μηχανικής [11]

Οι επιθέσεις Κοινωνικής Μηχανικής, μπορούν να διαχωριστούν σε τρεις κατηγορίες, αναλόγως με τον τρόπο που διεξάγονται ως ακολούθως:



Σχήμα 2.1: Κατηγορίες Κοινωνικής Μηχανικής

Οι κατηγορίες αυτές, αναλύονται:

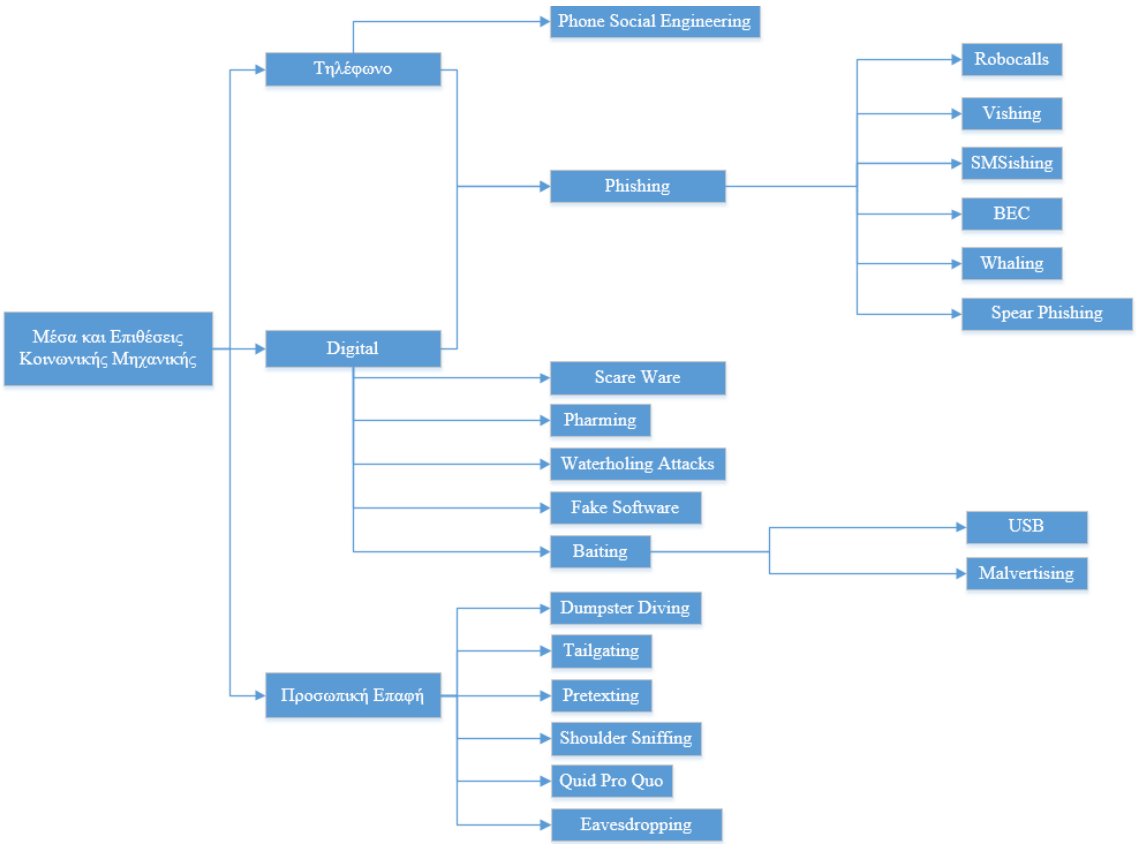
- Μέσω Τηλεφώνου: Στη κατηγορία αυτή, κατατάσσονται οι επιθέσεις τύπου Smishing, Vishing, Robocalls και Phone Social Engineering Attacks. Κατά τις επιθέσεις αυτές ο επιτιθέμενος επικοινωνεί με τα θύματα του με τη χρήση συσκευής τηλεφώνου, μέσω γραπτού μηνύματος, μέσω τηλεφωνικής κλήσης είτε ηχογραφημένου μηνύματος. Σκοπός σε κάθε περίπτωση είναι η συλλογή προσωπικών πληροφοριών και στοιχείων.
- Digital Attacks: Οι επιθέσεις αυτές επιτυγχάνονται με τη χρήση μέσων όπως είναι τα emails, λογισμικά προγράμματα, ψεύτικες ιστοσελίδες και εξωτερικές μονάδες

αποθήκευσης. Σκοπός είναι να δελεάσουν το χρήστη να χρησιμοποιήσει κάποιο από αυτά τα μέσα τα οποία στη συνέχεια θα τον παραπλανήσουν για να αποσπάσουν σημαντικές πληροφορίες.

- Προσωπική Επαφή: Κατά τις επιθέσεις προσωπικής επαφής, ο επιτιθέμενος έχει άμεση επαφή με το θύμα και προσπαθεί με διάφορους τρόπους να συλλέξει πληροφορίες και προσωπικά δεδομένα, είτε να αποκτήσει πρόσβαση σε μέρη στα οποία δεν είναι εξουσιοδοτημένος.

2.1 Είδη Επιθέσεων Κοινωνικής Μηχανικής

Τα είδη των κοινωνικών επιθέσεων ποικίλουν και το κάθε ένα από αυτά, χρησιμοποιεί διαφορετικό τρόπο παραπλάνησης και συλλογής πληροφοριών από τα θύματα. Επιθέσεις όπως Phishing, Baiting, Pretexting, Tailgating, Dumpster Diving, Shoulder Sniffing, Quid Pro Quo, Robocalls, Phone Social Engineering, Pharming, SMSishing, Malvertising και Whaterholing attacks αποτελούν παραδείγματα από τα είδη επιθέσεων τα οποία και παρουσιάζονται στο σχήμα που ακολουθεί:



Σχήμα 2.2: Διάγραμμα Επιθέσεων Κοινωνικής Μηχανικής

2.1.1 Περιγραφή Επιθέσεων Κοινωνικής Μηχανικής

Baiting → Οι επιθέσεις Baiting (Δολώματος) θεωρούνται είδος επίθεσης Κοινωνικής Μηχανικής κατά στο οποίο γίνεται χρήση δολώματος με σκοπό οι επιτιθέμενοι να παρασύρουν το θύμα σε μια παγίδα προκειμένου να συλλέξουν χρήσιμες πληροφορίες όπως είναι τα διαπιστευτήρια μιας σύνδεσης είτε να εγκαταστήσουν ένα κακόβουλο λογισμικό. Αυτό το είδος επίθεσης, μπορεί να γίνει μέσα από 2 διαφορετικές μεθόδους.

- Η πρώτη μέθοδος είναι με τη χρήση διαδικτυακών διαφημίσεων και ενός διαδικτυακού συνδέσμου στον οποίο οι χρήστες καλούνται να επισκεφθούν προκειμένου να επωφεληθούν υπηρεσίες ή αγαθά. Η παραπλάνηση επιτυγχάνεται μέσα από ψευδής αναφορές όπως δωρεάν λήψεις μουσικής ή ταινιών, βραβεία και δώρα προκειμένου να δελεάσει τον χρήστη να επισκεφθεί την εν λόγο ιστοσελίδα. [12]
- Κατά την δεύτερη μέθοδο, οι επιθέσεις δολώματος δεν περιορίζονται στον ψηφιακό κόσμο, αλλά μπορούν να επιτευχθούν εκτός σύνδεσης με τη χρήση αποθηκευτικών μέσων όπως είναι οι εξωτερικοί σκληροί δίσκοι (External Disk), flash driver (USB) και φορητοί υπολογιστές. Οι συσκευές αυτές μένουν εκτεθειμένες σε ανοιχτό μέρος προκειμένου να κινήσουν την περιέργεια για χρήση από τα θύματα. [12]

Χαρακτηριστικό παράδειγμα επίθεσης δολώματος, θεωρείται η επίθεση που καταγράφηκε από τον Steve Stasiukonis το 2006 ιδρυτής της Secure Network Technologies, με σκοπό να αποκτήσει πρόσβαση σε πληροφορίες πελατών. Κατά την επίθεση, ο Steve και η ομάδα του χρησιμοποίησαν μονάδες USB οι οποίες ήταν μολυσμένες με έναν ιό τύπου Trojan. Στη συνέχεια, τα διασκόρπισε γύρω από το πάρκινγκ του οργανισμού έτσι ώστε να τραβήξουν την προσοχή των υπαλλήλων. Πολλοί από αυτούς, συνέδεσαν τα USB στους υπολογιστές τους, ενεργοποιώντας έτσι ένα κακόβουλο λογισμικό μέσα από το οποίο ο Steve απέκτησε πρόσβαση σε ορισμένα διαπιστευτήρια σύνδεσης υπαλλήλων. [13]

Pretexting → Οι επιθέσεις Pretexting είναι βασισμένες σε διάφορες προφάσεις οι οποίες παροτρύνουν το θύμα να δείξει εμπιστοσύνη στον επιτιθέμενο και γίνονται με τη χρήση ψεύτικων και πειστικών σεναρίων με απώτερο σκοπό την κλοπή προσωπικών πληροφοριών [03].

Σε αυτούς τους τύπους επιθέσεων, ο απατεώνας συνήθως υποδύεται μια αξιόπιστη οντότητα ή άτομο και παρουσιάζει ένα πρόβλημα όπου χρειάζονται στοιχεία από τον χρήστη για να

επιβεβαιώσει την ταυτότητά του. Εάν το θύμα δεν αντιληφθεί το κίνδυνο και δώσουν τα στοιχεία, οι εισβολείς διαπράττουν κλοπή ταυτότητας ή χρησιμοποιούν τα δεδομένα για τη διεξαγωγή κακόβουλων δραστηριοτήτων. Μια πιο προηγμένη τακτική του Pretexting περιλαμβάνει την εξαπάτηση των θυμάτων έτσι ώστε να προβούν σε ενέργειες που παρακάμπτουν τις πολιτικές ασφαλείας του οργανισμού. Για παράδειγμα, ένας εισβολέας παρουσιάζεται ως εξωτερικός ελεγκτής υπηρεσιών πληροφορικής, έτσι ώστε η ομάδα φυσικής ασφάλειας του οργανισμού να τον αφήσει να εισέλθει στο κτίριο.

Οι επιθέσεις γίνονται με τη δημοσίευση πληροφοριών σε μέρη όπως τηλεφωνικούς καταλόγους, δημόσιες ιστοσελίδες ή συνέδρια. Το πρόσχημα που χρησιμοποιείται μπορεί να αφορά προσφορά μιας υπηρεσίας είτε μια αγγελία για εργασία, μέσα από τις οποίες γίνονται ερωτήσεις συλλέγοντας έτσι προσωπικές πληροφορίες.

Tailgating → Οι επιθέσεις Tailgating (επιθέσεις ουράς), θεωρούνται οι επιθέσεις όπου ένα μη εξουσιοδοτημένο άτομο αποκτά φυσική πρόσβαση σε μια τοποθεσία στην οποία δεν έχει εξουσιοδότηση να εισέλθει. Αυτό επιτυγχάνεται ακολουθώντας κάποιον που έχει την άδεια για να εισέλθει σε αυτό το μέρος. Για παράδειγμα, ένας εισβολέας ζητά από ένα θύμα να κρατήσει την πόρτα ανοιχτή είτε να του επιτρέψει την είσοδο στο χώρο χρησιμοποιώντας ως δικαιολογία ότι ξέχασε την ταυτότητα της εταιρείας ή την κάρτα RFID (αναγνώριση ραδιοσυχνοτήτων). [03]

Dumpster Diving → Ως Dumpster Diving, θεωρείται η επίθεση στην οποία γίνεται μια έρευνα στο χώρο απορριμμάτων του θύματος με στόχο να βρεθούν ευαίσθητες πληροφορίες και να χρησιμοποιηθούν στη συνέχεια. Σε μια επίθεση Dumpster Diving, γίνεται συλλογή εγγράφων από τους κάδους τα οποία πιθανόν να περιλαμβάνουν ευαίσθητες πληροφορίες είτε στοιχεία όπως κωδικοί πρόσβασης, emails προσωπικές πληροφορίες και άλλα. Επιπρόσθετα, αυτού του είδους επίθεση, μπορεί να γίνει με τη συλλογή εξοπλισμού που χρησιμοποιείται από έναν χρήστη, όπως παλιά υλικά υπολογιστών, μονάδες δίσκου, CD και DVD στα οποία περιέχονται εξίσου σημαντικές πληροφορίες [14].

Shoulder Surfing → Η επίθεση Shoulder Surfing, ορίζεται ο τρόπος επίθεσης με τον οποίο ένας επιτιθέμενος έχει οπτική επαφή με την οθόνη του θύματος και το πληκτρολόγιο του με σκοπό να λάβει σημαντικές πληροφορίες οι οποίες καταχωρούνται ή εμφανίζονται. Αυτό μπορεί να επιτευχθεί με την παρακολούθηση του θύματος κατά την ώρα εισαγωγής κωδικών πρόσβασης ή ευαίσθητων πληροφοριών συλλέγοντας τα δεδομένα κατά την ώρα καταχώρησης τους. [03]

Quid Pro Quo → Ο όρος Quid Pro Quo, ορίζεται ως κάτι που δίνεται ή λαμβάνεται και έχει ως αντάλλαγμα κάτι άλλο. Ως μορφή Κοινωνικής Μηχανικής, μια επίθεση quid pro quo υπόσχεται μια συγκεκριμένη υπηρεσία σε αντάλλαγμα πληροφορίες που παρέχει ένας χρήστης. Ένα παράδειγμα μπορεί να θεωρηθεί όταν ο εισβολέας καλεί τηλεφωνικός το θύμα προσποιούμενος ότι είναι εκπρόσωπος τεχνικής υποστήριξης υπηρεσιών. Με τον τρόπο αυτό ο επιτιθέμενος αρχικά θα προσπαθήσει να πείσει το θύμα για το ποιος υποστηρίζει ότι είναι και στη συνέχεια θα ζητήσει προσωπικές πληροφορίες και στοιχεία [14].

Scareware → Οι επιθέσεις τύπου Scareware, θεωρείται μια τακτική κυβερνοεπίθεσης με στόχο να τρομοκρατήσει τους χρήστες με τη χρήση διαφόρων επιχειρημάτων έτσι ώστε να επισκεφθούν πλαστογραφημένες ή μολυσμένες ιστοσελίδες ή να χρησιμοποιήσουν κακόβουλο λογισμικό. Αναλυτικότερα, το Scareware είναι ένας τύπος επίθεσης κακόβουλου λογισμικού που ισχυρίζεται ότι έχει εντοπίσει έναν ιό ή άλλο ζήτημα σε μια συσκευή και κατευθύνει τον χρήστη να κατεβάσει ή να αγοράσει κακόβουλο λογισμικό για να επιλύσει το πρόβλημα. Σε γενικές γραμμές, το scareware είναι η πύλη για μια πιο περίπλοκη κυβερνοεπίθεση και όχι μια επίθεση από μόνη της. [15]

Phone Social Engineering → Σε αυτό τον τύπο επιθέσεων, ο εισβολέας επικοινωνεί με το θύμα μέσω τηλεφώνου αναζητώντας συγκεκριμένες πληροφορίες με στόχο να επηρεάσουν το θύμα ώστε να παραχωρήσει στοιχεία και προσωπικές πληροφορίες. Αυτό επιτυγχάνεται μέσω παραπλάνησης, υπόσχοντας στο θύμα κάποιο δωρεάν αγαθό ή δωρεάν προϊόντα. [03]

Fake Software → Οι επιθέσεις Fake Software (Ψεύτικου Λογισμικού), βασίζονται σε κακόβουλα λογισμικά ή ιστοσελίδες που έχουν σκοπό να ξεγελούν τα θύματα θεωρώντας ότι είναι γνωστά και αξιόπιστα. Το θύμα με τη σειρά του εισάγει σε αυτά στοιχεία όπως είναι πληροφορίες σύνδεσης, παραχωρώντας έτσι στον εισβολέα τα διαπιστευτήρια του. Έπειτα ο επιτιθέμενος τα χρησιμοποιεί στον νόμιμο ιστότοπο ή λογισμικό, αποκτώντας με αυτό τον τρόπο πρόσβαση. Συνήθως, οι ιστοσελίδες αυτές, μοιάζουν με τη σελίδα σύνδεσης ενός δημοφιλούς ιστότοπου που συνήθως επισκέπτεται το θύμα, όπως η μια τραπεζική ιστοσελίδα, το Facebook ή το Twitter [3], όπου τα θύματα εισάγουν τα στοιχεία σύνδεσης τους. Ο κακόβουλος χρήστης εκμεταλλεύεται την εμπιστοσύνη που έχουν τα θύματα για αυτούς τους ιστότοπους και αποκτά πρόσβαση στις πληροφορίες διαπιστευτηρίων τους [17].

Pharming → Στην επίθεση αυτή στόχος είναι ο χρήστης κατά την επίσκεψη του σε ένα συγκεκριμένο ιστότοπο να μεταφερθεί σε έναν άλλο ψεύτικο ιστότοπο προκειμένου να εισάγει πληροφορίες και προσωπικά δεδομένα [18]. Αυτή η επίθεση λειτουργεί παραβιάζοντας τον διακομιστή συστήματος ονομάτων τομέα (DNS) και εκμεταλλευόμενη τυχόν ευπάθειες για την αλλαγή της διεύθυνσης πρωτοκόλλου Διαδικτύου (IP) του κεντρικού υπολογιστή και του διακομιστή.

Eavesdropping → Σε μια επίθεση τύπου Eavesdroping, ο εισβολέας προσπαθεί να συλλέξει πληροφορίες μέσα από τις συνομιλίες που γίνονται μεταξύ ατόμων είτε εντός των εγκαταστάσεων ενός οργανισμού είτε σε δημόσιους χώρους όπως μπαρ και εστιατόρια. Πληροφορίες μπορούν επίσης να ληφθούν με την τοποθέτηση συσκευών παρακολούθησης εντός της ενός οργανισμού. [19]

Waterholing attack → Σε μια επίθεση Waterholing, ο επιτιθέμενος μετά από μια έρευνα αναφορικά με το ποιες ιστοσελίδες επισκέπτεται ένας χρήστης ή χρησιμοποιεί ένας οργανισμός, παραβιάζει τον ιστότοπο και μολύνει έναν ή περισσότερους από αυτούς με κακόβουλο λογισμικό. Αυτό γίνεται μέχρις ότου ο χρήστης ή κάποιο μέλος του οργανισμού δεν υποψιαστεί την παγίδα που έχει στηθεί και χρησιμοποιήσει την ιστοσελίδα.

Phishing → Προβαίνοντας σε μια περαιτέρω ανάλυση των επιθέσεων Κοινωνικής Μηχανικής, διαπιστώνεται ότι οι επιθέσεις Phishing, αποτελούνται από διάφορα άλλα είδη επιθέσεων όπως: [20]

- Spear phishing
- Whaling
- BEC
- Vishing
- Smishing
- Robocalls

Spear Phishing → Οι επιθέσεις Spear Phishing, γίνονται μέσω μηνυμάτων τα οποία είναι εξατομικευμένα με βάση τις δημόσιες πληροφορίες που έχει βρει ο εισβολέας για κάποιον παραλήπτη. Αρχικά, ο εισβολέας προβαίνει σε μια έρευνα για το στόχο του κατά την οποία θα συλλέξει διευθύνσεις email και οργανογράμματα για να κατανοήσει καλύτερα τον τρόπο

λειτουργίας του στόχου ή ενός οργανισμού και τους υψηλά προνομιούχους στόχους που θα μπορούσαν να έχουν απεριόριστη πρόσβαση σε σημαντικά δεδομένα.

Δηλαδή, μπορεί να περιλαμβάνει θέματα που αφορούν την τεχνογνωσία του παραλήπτη, τον ρόλο του σε έναν οργανισμό, τα ενδιαφέροντα του, καθώς επίσης και διάφορες άλλες πληροφορίες που μπορούν να αντλήσουν οι εισβολείς από τα κοινωνικά δίκτυα. Αυτές οι συγκεκριμένες λεπτομέρειες κάνουν το email να παρουσιάζεται νόμιμο και αυξάνουν τις πιθανότητες ο παραλήπτης να αποπλανηθεί και να εισέλθει σε συνδέσμους ή να προβεί εν αγνοία σε λήψη ενός κακόβουλου λογισμικού για να δώσει στον εισβολέα πρόσβαση στο σύστημα υπολογιστή του χρήστη και παράλληλα σε άλλες ευαίσθητες πληροφορίες. [21]

Το επόμενο βήμα είναι η δημιουργία μηνύματος ηλεκτρονικού ταχυδρομείου. Το μήνυμα μπορεί να περιέχει έναν σύνδεσμο για έναν ιστότοπο που ελέγχεται από τους εισβολείς ή έναν σύνδεσμο για λήψη λογισμικού. Πολλά από τα μηνύματα αυτά, χρησιμοποιούν ονόματα γνωστών οργανισμών για να αυξήσουν την πιθανότητα επιτυχίας. Ονόματα εταιριών όπως PayPal, Amazon, Google και Microsoft χρησιμοποιούνται σε ένα ηλεκτρονικό μήνυμα δίνοντας έτσι στους χρήστες μια αίσθηση εμπιστοσύνης με σκοπό να εξαπατηθούν και να εισέλθουν σε συνδέσμους από ένα email.

Whaling → Είναι μέθοδος επίθεσης κατά την οποία οι εγκληματίες του κυβερνοχώρου παρουσιάζονται ως άτομα που κατέχουν ανώτερη θέση σε έναν οργανισμό και στοχεύουν άμεσα σημαντικά άτομα, με στόχο την κλοπή χρημάτων, ευαίσθητων πληροφοριών ή την απόκτηση πρόσβασης σε συστήματα υπολογιστών. Κατά τις επιθέσεις Whaling, γίνεται χρήση μεθόδων όπως η πλαστογράφηση email και ιστότοπου για να εξαπατήσουν τον χρήστη με σκοπό να εκτελέσει συγκεκριμένες ενέργειες. [22]

Vishing → Οι επιθέσεις Vishing εκτελούνται μέσω τηλεφώνου και θεωρούνται ένας τύπος επιθέσεων Κοινωνικής Μηχανικής, όπου χρησιμοποιείται ο ψυχολογικός παράγοντας για να ξεγελάσουν τα θύματα, με σκοπό να παρέχει προσωπικές, οικονομικές ή άλλες εμπιστευτικές πληροφορίες [03]. Ένα χαρακτηριστικό παράδειγμα επίθεσης Vishing, το οποίο είναι ευρέως διαδεδομένο στις ΗΠΑ, θεωρείται όταν ο επιτιθέμενος τηλεφωνεί με σκοπό να εισπράξει απλήρωτους φόρους προειδοποιώντας παράλληλα τα θύματα ότι απειλούνται με ποινή φυλάκισης. Με αυτό τον τρόπο απειλής, ο φόβος της σύλληψης μπορεί να προκαλέσει τα θύματα να δώσουν όλες τις πληροφορίες που ζητεί ο επιτιθέμενος.

Robocalls → Οι ρομποτικές επιθέσεις εμφανίστηκαν πρόσφατα και αποτελούν μαζικές κλήσεις σε κινητά τηλέφωνα, σε οικίες και σε τηλέφωνα εργασίας που προέρχονται από υπολογιστές και έχουν ως αποδέκτες άτομα με γνωστούς αριθμούς τηλεφώνου. Σύμφωνα με την εταιρεία Kaspersky, μια αυτοματοποιημένη κλήση που παραδίδει μηνύματα, τα οποία είναι ήδη ηχογραφημένα μέσω λογισμικού αυτόματης κλήσης σε εκατομμύρια ανθρώπους κάθε μέρα παρέχουν χρήσιμες πληροφορίες, όπως υπενθυμίσεις ραντεβού, ακυρώσεις πτήσεων, είτε προσπαθούν να πείσουν τα θύματα τους να προβούν σε συγκεκριμένες αγορές προϊόντων. Εναλλακτικά, αυτές οι κλήσεις μπορεί να προωθούν την προσφορά ή την πώληση υπηρεσιών για την επίλυση προβλημάτων με στόχο να πείσει το θύμα για την αποστολή χρήματων ή προσωπικών πληροφοριών. Αυτού του είδους επιθέσεις, μπορούν εύκολα να πραγματοποιηθούν μέσω του διαδικτύου χωρίς να έχουν ιδιαίτερο κόστος, κάτι που τις επιτρέπει να είναι τόσο διαδεδομένες. [23]

BEC → (Business email compromise) Θεωρούνται οι επιθέσεις που επιτυγχάνονται μέσω emails και συγκεκριμένα απειλώντας τους οργανισμούς ως μέρος των τυπικών διαδικασιών τους. Οι επιθέσεις BEC συνήθως ξεκινούν με έναν από τους δύο ακόλουθους τρόπους:

- βάζοντας έναν ανυποψίαστο υπάλληλο να εισέλθει σε ένα συνημμένο ηλεκτρονικό μήνυμα που θέτει σε κίνδυνο το δίκτυο
- στέλνοντας ένα ηλεκτρονικό μήνυμα που υποδύεται έναν υψηλόβαθμο αξιωματούχο της εταιρείας.

Ο δράστης δημιουργεί ένα ψεύτικο ηλεκτρονικό μήνυμα όμοιο με το email της εταιρείας του θύματος, μέσω του οποίου αποστέλνονται μηνύματα τα οποία απευθύνονται στο προσωπικό της εταιρείας σε μια προσπάθεια να αποκτήσουν αριθμούς λογαριασμού, κωδικούς πρόσβασης ή άλλες ευαίσθητες πληροφορίες. [24] Στις επιθέσεις BEC, η Κοινωνική Μηχανική είναι ένα κεντρικό στοιχείο στο οποίο οι εγκληματίες του κυβερνοχώρου καταγράφουν μεγάλη αποτελεσματικότητα στην εξαπάτηση εταιρειών και εργαζομένων σε όλο τον κόσμο, γεγονός που επιτρέπει να χρησιμοποιείται όλο και περισσότερο εφόσον είναι επιτυχής και δύσκολο να εξεταστεί ή να αντιμετωπιστεί. [25]

SMishing → Οι επιθέσεις SMishing γίνονται με την αποστολή μηνυμάτων κειμένου σε κινητά τηλέφωνα στα θύματα με σκοπό να τα επηρεάσουν για να αποκτήσουν πληροφορίες. Η αποτελεσματικότητα των επιθέσεων SMishing έγκειται στο γεγονός ότι τα θύματα μπορούν να

μεταφέρουν τα κινητά τους τηλέφωνα οπουδήποτε και οποτεδήποτε. Ένα μήνυμα κειμένου που λαμβάνεται, μπορεί να περιλαμβάνει κακόβουλο λογισμικό, ακόμη κι αν έχει σταλεί από αξιόπιστο και γνωστό άτομο. Το κακόβουλο λογισμικό λειτουργεί ως διαδικασία παρασκηνίου με τρόπο έτσι ώστε να έχουν πρόσβαση οι εισβολείς σε πληροφορίες όπως λίστα επαφών, μηνύματα, προσωπικά email, φωτογραφίες, σημειώσεις, εφαρμογές και ημερολόγιο. Ακόμη καταγράφονται περιπτώσεις στις οποίες ο απατεώνας μπορεί να εγκαταστήσει ένα λογισμικό για τον πλήρη έλεγχο του κινητού τηλεφώνου [20].

2.2 Τρόποι Αντιμετώπισης Επιθέσεων Κοινωνικής Μηχανικής

Οι Επιθέσεις Κοινωνικής Μηχανικής, λόγω του ότι πολλές από αυτές είναι σχεδιασμένες να επηρεάζουν την ψυχολογία των ανθρώπων, θεωρούνται ιδιαίτερα δύσκολες να αντιμετωπιστούν. Για την αντιμετώπιση τους, υπάρχουν διάφορα μέτρα που προτείνονται να λαμβάνονται προκειμένου οι χρήστες και οι οργανισμοί να είναι ασφαλείς. Μερικά από αυτά περιλαμβάνουν τη χρήση ασφάλειας 2 παραγόντων, την συστηματική ενημέρωση και αναβάθμιση λογισμικών συστημάτων, τη διαδικασία καταγραφής αντιγράφων ασφαλείας, τον έλεγχο λογισμικών προγραμμάτων πριν από την εγκατάσταση τους, καθώς επίσης και έλεγχο μονάδων αποθήκευση όπως είναι τα USB πριν από τη χρήση τους.

Οι τρόποι αντιμετώπισης, μπορεί να διαχωριστούν σε διάφορες κατηγορίες, όπου προκύπτει ότι κάθε ένας τρόπος αντιστοιχεί για την αντιμετώπιση διαφόρων μορφών επιθέσεων.

Οι κατηγορίες μπορεί να χωριστούν σε:

- Θέματα προσβασιμότητας
- Εκπαίδευση
- Ενημέρωση
- Αντίγραφα ασφαλείας
- Λογισμικά Προγράμματα
- Αναβαθμίσεις

Προσπάθεια αποτροπής των επιθέσεων και ενημέρωση των πολιτών, γίνεται μέσα από τα Μέσα Μαζικής Ενημέρωσης, όπου συχνά γίνονται αναφορές για τρόπους επιθέσεων που βρίσκονται σε

έξαρση. Δελτία ειδήσεων, εφημερίδες και αναρτήσεις στο διαδίκτυο, ενημερώνουν και προτρέπουν για τους τρόπους που επιτήδειοι προσπαθούν να παραπλανήσουν πολίτες ενώ παράλληλα παρέχουν συμβουλές για μέτρα προστασίας.

Παράδειγμα ενημέρωσης είναι άρθρο από την ιστοσελίδα 'Reporter [26]', στο οποίο αναφέρεται απάτες που γίνονται σε Μέσα Κοινωνικής Δικτύωσης και ιδιαίτερα στο Instagram με τη χρήση μηνυμάτων. Συγκεκριμένα, οι χρήστες λαμβάνουν μήνυμα από γνωστά τους πρόσωπα στο Instagram και τους παροτρύνουν όπως επενδύσουν σε κρυπτονομίσματα. Τα μηνύματα αυτά είναι κακόβουλα και έχουν ως σκοπό το οικονομικό όφελος καθώς και να αποκτήσουν πρόσβαση στον λογαριασμό του παραλήπτη. Στο συγκεκριμένο άρθρο, συμπεριλαμβάνονται ορισμένες συστάσεις προς τους χρήστες, παρέχοντας έτσι τη δυνατότητα για προστασία. Μέσα από τις συστάσεις, προτρέπονται οι χρήστες να είναι προσεκτικοί σε μηνύματα που λαμβάνουν και να μην αποκαλύπτουν προσωπικές πληροφορίες. Επιπρόσθετα, προτείνεται η χρήση ασφαλείας 2 παραγόντων, καθώς επίσης η εξακρίβωση του μηνύματος που λήφθηκε επικοινωνώντας με κάποιο άλλο πρόσωπο. Για περιπτώσεις όπου ο χρήστης εξαπατήθηκε και προέβη σε ενέργειες που του υποδείχτηκαν, συνίσταται όπως γίνει άμεση αλλαγή κωδικού πρόσβασης σε όλους τους λογαριασμούς.

Σε διαφορετικό άρθρο [27] της ίδιας ιστοσελίδας, γίνεται αναφορά σε ηλεκτρονικά μηνύματα που αποστέλνονται και φέρουν το λογότυπο της Αστυνομίας, απειλώντας μέσα από αυτά τους πολίτες με καταγγελίες. Συγκεκριμένα, γίνεται αναφορά σε παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία αποστέλλονται μαζικά στο κοινό και παριστάνουν ψευδώς ότι προέρχονται από την Αστυνομία, αναφέροντας στα θύματα ότι είναι εμπλεκόμενοι και πρέπει να κατηγορηθούν για διάφορα ποινικά αδικήματα. Με τον τρόπο αυτό, προκαλείται το αίσθημα του εκφοβισμού και οι αποστολείς των μηνυμάτων, προσπαθούν να προκαλέσουν τους χρήστες να προβούν σε πληρωμή παράνομων αδικημάτων αποσπώντας έτσι χρηματικά ποσά.

Ο οργανισμός CIS – Center for Internet Security, ο οποίος είναι ανεξάρτητος μη κερδοσκοπικός οργανισμός με στόχο να επιφέρει την εμπιστοσύνη στον κόσμο του διαδικτύου, προτείνει διάφορα στοιχεία ελέγχου τα οποία θα συνδράμουν για την αντιμετώπιση των επιθέσεων και έχουν ως ακολούθως. [28]

Καταγραφή και έλεγχος περιουσιακών στοιχείων (Hardware and Software) της επιχείρησης – Προτείνεται η καταγραφή και ο έλεγχος όλων των περιουσιακών στοιχείων, όπως

είναι οι διακομιστές (Servers), υπολογιστές, κινητά τηλέφωνα και συσκευές δικτύου τα οποία χρησιμοποιούνται από τα ανάλογα άτομα, καθώς επίσης και όλα τα λογισμικά συστήματα που χρησιμοποιούνται τόσο εντός του δικτύου όσο και εκτός. Έτσι ο οργανισμός θα έχει το σύνολο των περιουσιακών στοιχείων που πρέπει να παρακολουθούνται και να προστατεύονται εντός της επιχείρησης καθώς επίσης και στον εντοπισμό μη εξουσιοδοτημένων και μη διαχειριζόμενων περιουσιακών στοιχείων. Επιπρόσθετα, μπορεί να εντοπιστεί ή να αποτραπεί εγκατάσταση μη εξουσιοδοτημένου λογισμικού το οποίο θα μπορούσε να χρησιμοποιηθεί κακόβουλα.

Προστασία δεδομένων - Προτρέπετε η ανάπτυξη διαδικασιών και τεχνικών ελέγχων για τον εντοπισμό, την ταξινόμηση, τον ασφαλή χειρισμό, τη διατήρηση και τη διαθεσιμότητα των δεδομένων.

Ασφαλής διαμόρφωση περιουσιακών στοιχείων και λογισμικού της επιχείρησης – Δημιουργία και διατήρηση της ασφαλής διαμόρφωσης των περιουσιακών στοιχείων της επιχείρησης σχετικά με τις συσκευές και τα λογισμικά που χρησιμοποιούνται.

Διαχείριση λογαριασμού – Προτείνεται η χρήση εργαλείων για την ταξινόμηση, τον διαχωρισμό και την διαχείριση εξουσιοδότησης για λογαριασμούς των χρηστών, του διαχειριστή καθώς και των υπηρεσιών γενικότερα.

Διαχείριση Ελέγχου Πρόσβασης - Χρήση εργαλείων για την δημιουργία, την εκχώρηση και τη διαχείριση λογαριασμών χρηστών, καθώς επίσης και η διαχείριση ελέγχου πρόσβασης σε ένα σημαντικό μέρος όπου κρίνεται αναγκαίο .

Συνεχής Διαχείριση Ευπαθειών – Με το ένα σχέδιο αυτό επιτυγχάνεται η συνεχής αξιολόγηση και παρακολούθηση των τρωτών σημείων στα περιουσιακά στοιχεία της επιχείρησης εντός της υποδομής, προκειμένου να ελαχιστοποιηθεί ή ακόμη και να αποκατασταθεί τυχόν ευπάθειες που υπάρχουν.

Διαχείριση αρχείων καταγραφής ελέγχου – Η διαδικασία καταγραφής ελέγχου, γίνεται με σκοπό την τεκμηρίωση μιας δραστηριότητας που έλαβε χώρα στα συστήματα λογισμικού ενός οργανισμού και καταγράφεται η εμφάνιση ενός συμβάντος, η στιγμή που συνέβη, τον υπεύθυνο χρήστη ή την υπηρεσία και την επηρεαζόμενη οντότητα. Τα αρχεία καταγραφής ελέγχου συμβάντων μπορούν να συμβάλουν στον εντοπισμό, την κατανόηση ή την ανάκτηση μιας επίθεσης.

Email και Προστασία προγράμματος περιήγησης στο Web – Τα ηλεκτρονικά μηνύματα, θεωρούνται ως τα κύρια μέσα αλληλεπίδρασης των χρηστών με εξωτερικούς μη αξιόπιστους χρήστες και περιβάλλοντα μέσα από τα οποία μπορούν να γίνουν προσπάθειες για επιθέσεις Κοινωνικής Μηχανικής. Για το λόγω αυτό, θεωρείται απαραίτητο να λαμβάνονται προστασίες για τον εντοπισμό απειλών από φορείς ηλεκτρονικού ταχυδρομείου και ιστού, καθώς αυτές είναι ευκαιρίες για τους εισβολείς να χειραγωγήσουν την ανθρώπινη συμπεριφορά μέσω άμεσης εμπλοκής.

Άμυνας από κακόβουλο λογισμικό - Αποτρέψτε ή ελέγξτε την εγκατάσταση, τη διάδοση και την εκτέλεση κακόβουλων εφαρμογών, κώδικα ή σεναρίων σε εταιρικά στοιχεία.

Ανάκτηση δεδομένων – Θεωρείται απαραίτητη η διατήρηση επαρκών πρακτικών για σκοπό ανάκτησης δεδομένων και την επαναφορά των περιουσιακών στοιχείων της επιχείρησης σε περίπτωση συμβάντος που θα επιφέρει την διαγραφή / καταστροφή δεδομένων.

Διαχείριση υποδομής δικτύου - Δημιουργήστε, εφαρμόστε και διαχειριστείτε ενεργά (παρακολούθηση, αναφορά, διόρθωση) συσκευών δικτύου, προκειμένου να αποτρέψετε τους εισβολείς να εκμεταλλευτούν ευάλωτες υπηρεσίες δικτύου και σημεία πρόσβασης.

Παρακολούθηση και άμυνα δικτύου - Λειτουργία διαδικασιών και εργαλείων έτσι ώστε να γίνεται δημιουργία και διατήρηση μιας ολοκληρωμένης παρακολούθησης του δικτύου ενός οργανισμού καθώς επίσης και των μέτρων άμυνας που λαμβάνονται έναντι απειλών ασφαλείας σε όλη την υποδομή δικτύου και τη βάση χρηστών της επιχείρησης.

Εκπαίδευση επίγνωσης και δεξιοτήτων ασφάλειας – Ο ανθρώπινος παράγοντας θεωρείται ίσως ο σημαντικότερος και πιο ο ευάλωτος για την επίτευξη μιας επίθεσης Κοινωνικής Μηχανικής. Το γεγονός αυτό οδηγεί στο συμπέρασμα ότι η εκπαίδευση και ενημέρωση των χρηστών και προσωπικού ενός οργανισμού είναι απαραίτητη. Συστήνεται η δημιουργία ενός προγράμματος ευαισθητοποίησης για την ασφάλεια με στόχο να επηρεαστεί η συμπεριφορά μεταξύ του εργατικού δυναμικού, ώστε να έχει επίγνωση της ασφάλειας και να είναι κατάλληλα καταρτισμένο για τη μείωση των κινδύνων στον κυβερνοχώρο για την επιχείρηση.

Διαχείριση παρόχου υπηρεσιών – Επιβάλλεται η ανάπτυξη διαδικασίας με σκοπό την αξιολόγηση σε όσους παρέχουν υπηρεσίες και κατέχουν ευαίσθητα δεδομένα ή είναι υπεύθυνοι

για συστήματα όπως λογισμικά προγράμματα, διακομιστές και διαδικασίες IT ενός οργανισμού, για να διασφαλιστεί ότι αυτοί οι πάροχοι προστατεύουν κατάλληλα αυτά τα δεδομένα.

Ασφάλεια λογισμικού εφαρμογής– Διαδικασία κατά την οποία γίνεται έλεγχος στα λογισμικά προγράμματα που χρησιμοποιούνται με σκοπό την πρόληψη, τον εντοπισμό και την αποκατάσταση αδυναμιών ασφάλειας προτού αυτά χρησιμοποιηθούν.

Απόκριση και διαχείριση περιστατικών – Η απόκριση και διαχείριση περιστατικών, είναι η στρατηγική που επιτρέπει έναν οργανισμό να αντιμετωπίζει περιστατικά κυβερνοασφάλειας και παραβίαση της ασφάλειας. Αυτό επιτυγχάνεται με τον έλεγχο της κατάστασης, τον περιορισμός της ζημιάς που προκαλείται από έναν εισβολέα και η μείωση του χρόνου και του κόστους ανάκτησης το οποίο γίνεται με την καθιέρωση ενός προγράμματος για την ανάπτυξη και τη διατήρηση μιας ικανότητας απόκρισης περιστατικού που θα περιλαμβάνει πολιτικές, σχέδια, διαδικασίες, καθορισμένοι ρόλοι, εκπαίδευση και επικοινωνίες για την προετοιμασία, τον εντοπισμό και την ταχεία απόκριση σε μια επίθεση.

Δοκιμές Διείσδυσης – Θεωρείται μια εξουσιοδοτημένη προσομοίωση επίθεσης σε ένα σύστημα, η οποία εκτελείται με σκοπό την αξιολόγηση της ασφάλειας ενός συστήματος. Με τη διαδικασία αυτή δοκιμάζετε η αποτελεσματικότητα και η ανθεκτικότητα των περιουσιακών στοιχείων της επιχείρησης από τυχόν αδυναμίες καθώς επίσης και εντοπισμός των στόχων και των ενεργειών ενός εισβολέα. [28]

Στον πίνακα που ακολουθεί, παρουσιάζονται οι τρόποι αντιμετώπισης επιθέσεων, τα είδη επιθέσεων που αντιμετωπίζονται με κάθε ένα τρόπο καθώς επίσης και τα άτομα που είναι αρμόδια για την υλοποίηση της αντιμετώπισης:

Τρόποι αντιμετώπισης	Επιθέσεις που αντιμετωπίζονται
Καταγραφή και έλεγχος περιουσιακών στοιχείων οργανισμού	Tailgating Pretexting Quid Pro Quo Dumpster Diving
Καταγραφή και έλεγχος περιουσιακών στοιχείων λογισμικού	Baiting Quid Pro Quo
Προστασία δεδομένων	Phone Social Engineering Pretexting Phishing Quid Pro Quo Dumpster Diving
Ασφαλής διαμόρφωση περιουσιακών στοιχείων και λογισμικού της επιχείρησης	Pretexting Baiting
Διαχείριση λογαριασμού	Baiting
Διαχείριση Ελέγχου Πρόσβασης	Tailgating Shoulder Sniffing Pretexting
Συνεχής Διαχείριση Ευπαθειών	Phishing Scare Ware
Διαχείριση αρχείων καταγραφής ελέγχου	Tailgating
Email και Προστασία προγράμματος περιήγησης στο Web	Waterholing Attacks Phishing Fake Software Scare Ware
Άμυνας κακόβουλου λογισμικού	Phishing Fake Software Scare Ware
Ανάκτηση δεδομένων	Shoulder Sniffing Phishing
Διαχείριση υποδομής δικτύου	Waterholing Attacks Phishing
Παρακολούθηση και Άμυνα Δικτύου	Waterholing Attacks Phishing Fake Software

Εκπαίδευση επίγνωσης και δεξιοτήτων ασφάλειας	Waterholing Attacks Shoulder Sniffing Social Engineering Pharming Baiting Phishing Fake Software Scare Ware
Ασφάλεια λογισμικού εφαρμογής	Baiting Phishing Fake Software Scare Ware
Απόκριση και διαχείριση περιστατικών	Dumpster Diving

Πίνακας 2.1: Επιθέσεις Κοινωνικής Μηχανικής και Τρόποι Αντιμετώπισης

2.3 Εκπαιδευτικές Δραστηριότητες για Αντιμετώπιση Κοινωνικής Μηχανικής

Η ενημέρωση και εκπαίδευση των πολιτών έναντι επιθέσεων Κοινωνικής Μηχανικής μέσα από μια δραστηριότητα, θεωρείται τρόπος με τον οποίο θα προσελκύει το ενδιαφέρον και θα αποδώσει στην κατανόηση και απομνημόνευση των κινδύνων των επιθέσεων.

The Social Engineer

Το παιχνίδι 'The Social Engineer', δημιουργήθηκε με σκοπό την ευαισθητοποίησης των χρηστών σχετικά με την Κοινωνική Μηχανική και θεωρείται ένα παιχνίδι όπου οι παίχτες πρέπει να χρησιμοποιήσουν διάφορες μεθόδους επιθέσεων Κοινωνικής Μηχανικής με σκοπό να ανακτήσουν εμπιστευτικές πληροφορίες ή να αποκτήσουν πρόσβαση σε περιορισμένες τοποθεσίες εκμεταλλευόμενοι τον ανθρώπινο παράγοντα. Αυτό επιτυγχάνεται με τους ελέγχουν ασφαλείας που γίνονται από τους χρήστες σε μια προσομοιωμένη εταιρεία. Το παιχνίδι γίνεται με τη χρήσης της εικονικής πραγματικότητας και σε αυτό οι παίχτες έχουν την ευκαιρία σε διαφορετικές αποστολές να εφαρμόσουν διαφορετικές μεθόδους επίθεσης Κοινωνικής Μηχανικής.

Σε αυτό το παιχνίδι, κάθε αποστολή αποτελείται από διαφορετικά καθήκοντα και ολοκληρώνεται όταν έχουν αποκαλυφθεί ένα ή περισσότερα ελαττώματα ασφαλείας. Δηλαδή, σκοπός κάθε αποστολής είναι να ληφθούν πληροφορίες οι οποίες κανονικά δεν θα πρέπει να είναι προσβάσιμες

από άτομα που δεν εμπλέκονται με τον οργανισμό. Με την ολοκλήρωση κάθε μιας αποστολής, παρουσιάζεται μια επισκόπηση των τρωτών σημείων που έχουν ανευρεθεί, μαζί με συμβουλές για την αποφυγή επιθέσεων Κοινωνικής Μηχανικής με τη για την ενίσχυση του μαθησιακού αποτελέσματος.

Αν και το παιχνίδι παρέχει ένα φιλικό περιβάλλον προς τον χρήστη με διάφορα σενάρια για επιθέσεις κοινωνικής μηχανική, εντούτοις, δεν μπορεί να χρησιμοποιηθεί και να αξιοποιηθεί από όλους τους χρήστες εφόσον ο μηχανισμός για την εικονική πραγματικότητα θεωρείται απαραίτητος, κάτι όμως που έχει και ανάλογο κόστος. [29]

PlayingSafe

Το PlayingSafe είναι ένα παιχνίδι που δημιουργήθηκε για την αντιμετώπιση των επιθέσεων Κοινωνικής Μηχανικής. Αποτελείται από ένα πίνακα ο οποίος περιέχει 32 τετράγωνα, με το καθένα να αντιστοιχίζεται σε μια κατηγορία επίθεση Κοινωνικής Μηχανικής και καθορίζεται από διαφορετικό χρώμα στον πίνακα παιχνιδιού. Σε κάθε κατηγορία αντιστοιχούν ερωτήσεις πολλαπλής επιλογής οι οποίες αφορούν επιθέσεις Phishing, απάτη για καταβολή πληρωμών, ανεπιθύμητα μηνύματα και άλλες μεθόδους επιθέσεων Κοινωνικής Μηχανικής. Με κάθε απάντηση που δίνει ο χρήστης, συγκεντρώνεται βαθμολογία η οποία παρακολουθείται καθ' όλη τη διάρκεια του παιχνιδιού, προκειμένου να παρέχεται ένα επιπλέον επίπεδο κινήτρων στον χρήστη, και έτσι να αυξήσουν τις γνώσεις και την εκπαίδευσή τους. [30]

Persuaded

Το Persuaded, είναι ένα παιχνίδι που υλοποιήθηκε με σκοπό την αντιμετώπιση επιθέσεων Κοινωνικής Μηχανικής εφόσον έχει ως στόχο να εκθέσει τους ανθρώπους σε ρεαλιστικά σενάρια επιθέσεων. Σχεδιάστηκε έτσι ώστε να επιτευχθεί η αύξηση της ευαισθητοποίησης για την Κοινωνική Μηχανική, η κατάρτιση αντίστασης στις επιθέσεις και στις απειλές, καθώς επίσης και για να απευθύνεται και να μπορεί να χρησιμοποιηθεί από τον γενικό πληθυσμό ανεξαρτήτως ηλικία και γνώσεις. Το παιχνίδι δίνει τη δυνατότητα στους εργαζόμενους να ενημερωθούν για την Κοινωνική Μηχανική, ενώ παράλληλα μπορούν να εξασκηθούν σε τρόπους αντιμετώπισης γεγονός που παρέχει αποδεδειγμένα διαρκεί αποτελέσματα.

Οι χρήστες έρχονται αντιμέτωποι με ένα πιθανό σενάριο κοινωνικής απειλής και πρέπει να επιλέξουν έναν αμυντικό μηχανισμό ως τρόπο αντιμετώπισης έτσι ώστε να εξασφαλιστεί ένα

ασφαλές αποτέλεσμα. Για παράδειγμα, ο χρήστης λαμβάνει ένα μήνυμα ηλεκτρονικού ψαρέματος και όπου ζητείται να ανοίξει το συνημμένο αρχείο που περιέχει. Ακολούθως, ο χρήστης επιλέγει ένα τρόπο αντιμετώπισης, τον οποίο θεωρεί ως καταλληλότερο μέτρο και λαμβάνει άμεσα σχόλια αν η άμυνα που επιλέχθηκε είναι σωστή.

Θεωρείται ότι το Persuaded μπορεί να παρέχει εύκολη εκμάθηση εφόσον έχει χαμηλό επίπεδο πολυπλοκότητας γεγονός που το κάνει να είναι πιο ελκυστικό για τους αρχάριους χρήστες. Επιπρόσθετα, παρέχει μια ευκολία στο τρόπο παιχνιδιού έτσι ώστε να ενσωματωθεί εύκολα στην καθημερινή ρουτίνα των παικτών και να έχει ελάχιστη απαραίτητη προετοιμασία και σύντομο χρόνο κατά τη διεξαγωγή του. [31]

SEAG

Το SEAG είναι ένα παιχνίδι που έχει σχεδιαστεί για να αυξήσει την ευαισθητοποίηση σχετικά με τις επιθέσεις Κοινωνικής Μηχανικής. Το παιχνίδι χρησιμοποιεί επίπεδα που αντιμετωπίζουν διαφορετικές γνωστικές πτυχές και ως εκ τούτου παρέχουν μια αποτελεσματική μαθησιακή εμπειρία. Το πρώτο επίπεδο αποτελείται από ερωτήσεις τύπου κουίζ έτσι ώστε να δημιουργείται μια βάση γνώσεων για τους παίκτες. Το δεύτερο επίπεδο είναι ένα παιχνίδι αγώνα όπου οι χρήστες πρέπει να αντιστοιχίσουν τις μεθόδους Κοινωνικής Μηχανικής με τις αντίστοιχες εικόνες. Τελικό στάδιο, παρουσιάζονται σενάρια που αντιμετωπίζονται στην καθημερινότητα με σκοπό να αναλυθούν σχετικά με την ανάλογη απειλή, γεγονός που παρέχει την προσομοίωση της πραγματικής εφαρμογής της ζωής προκειμένου να δοκιμάσει τους χρήστες την ικανότητα ανίχνευσης και αντίληψης επιθέσεων. [32]

Κεφάλαιο 3

Μεθοδολογία

3.1 Εντοπισμός και Ανάλυση Δεδομένων

Στόχος της έρευνας είναι η συλλογή και ανάλυση δεδομένων προκειμένου να σχηματιστεί μια εικόνα για το πού εστιάζονται οι επιθέσεις Κοινωνικής Μηχανικής, ποιοι τρόποι επιθέσεων χρησιμοποιούνται και ποια άτομα ή οργανισμοί είναι στόχοι επιθέσεων. Στη συνέχεια, μετά από την ανάλογη μελέτη, αυτά τα στοιχεία θα βοηθήσουν στην υλοποίηση της εκπαιδευτικής δραστηριότητας.

Για την καλύτερη και αποτελεσματικότερη συγκρότηση στοιχείων, τέθηκαν τα εξής ερωτήματα σχετικά με το εν λόγο θέμα:

- Τι ορίζεται ως Κοινωνική Μηχανική;
- Ποιο είναι το πρόβλημα της Κοινωνικής Μηχανικής;
- Ποια τα στατιστικά στοιχεία επιθέσεων Κοινωνικής Μηχανικής
- Ποια είδη επιθέσεων εντοπίζονται κατά την Κοινωνική Μηχανική;
- Ποιες είναι οι ενημερωτικές δράσεις και ποια τα αποτελέσματα αναφορικά με τις επιθέσεις Κοινωνικής Μηχανικής;
- Ποιοι είναι οι τρόποι αντιμετώπισης των επιθέσεων Κοινωνικής Μηχανικής;
- Ποια είναι τα υπάρχοντα εκπαιδευτικά παιχνίδια αναφορικά με τις επιθέσεις Κοινωνικής Μηχανικής;

Η έρευνα για τον εντοπισμό των απαντήσεων έναντι αυτών των ερωτημάτων, έγινε μέσω της μηχανής αναζήτησης Google Scholar και IEEE, από όπου παρέχεται ένας απλός τρόπος αναζήτησης επιστημονικής βιβλιογραφίας, στον οποίο περιλαμβάνονται διαδικτυακά ακαδημαϊκά περιοδικά, βιβλία, εργασίες και διατριβές. Έγινε επίσης χρήση της πύλης MyAthens του ΑΠΚυ, καθώς και του εργαλείου Ενοποιημένης Αναζήτησης "TEFKROS".

Επιπρόσθετα, για τον εντοπισμό της βιβλιογραφίας, έγινε αναζήτηση άρθρων που έχουν δημοσιευθεί σε εγκεκριμένα επιστημονικά περιοδικά ή παρουσιαστεί σε συνέδρια τα τελευταία έτη.

Παράλληλα, έγινε η χρήση Google Books για ανεύρεση βιβλίων που παραπέμπουν σε αναφορές για την Κοινωνική Μηχανική, καθώς επίσης και διαδικτυακή έρευνα για τη συλλογή πληροφοριών και στοιχείων μέσα από εταιρείες και οργανισμούς που παρέχουν υπηρεσίες προστασίας και ασφάλειας δεδομένων.

Η έρευνα για την ενημερωτική δράση έναντι των επιθέσεων Κοινωνικής Μηχανικής, έγινε μέσα από τη διαδικτυακή πλατφόρμα της Αστυνομίας Κύπρου (https://cyberalert.cy/), καθώς επίσης και από ιστοσελίδες Μέσων Μαζικής Ενημέρωσης, προκειμένου να εντοπιστούν άρθρα που αναφέρονται σε επιθέσεις.

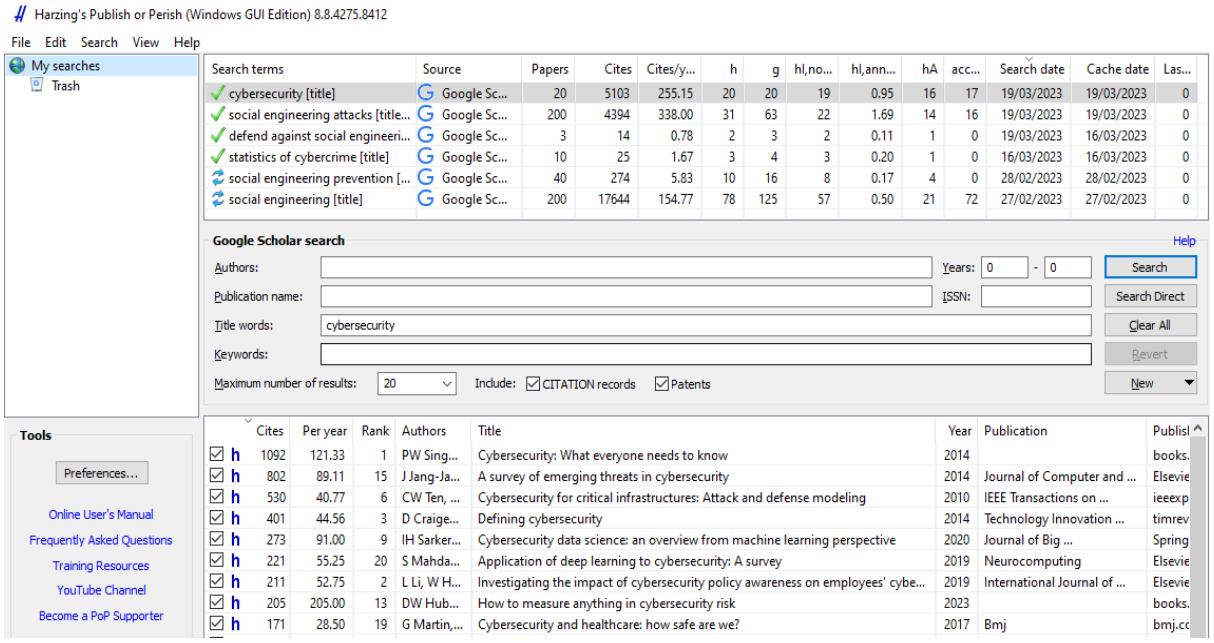
Η αναζήτηση των πιο πάνω έγινε με τη χρήση όρων και λέξης κλειδιών όπως:

- Social engineering
- Social Engineering Attack types
- Prevention against Social Engineering attacks
- Social Engineering Statistics
- Cybercrime
- Hacking
- Social Engineering Games
- Games against Social Engineering

Κατά την αναζήτηση έχει εντοπιστεί μεγάλος αριθμός από πηγές στοιχείων μέσα από επιστημονικά άρθρα, βιβλία, περιοδικά και ιστοσελίδες. Τα αποτελέσματα αυτά αξιολογήθηκαν με σκοπό την επιλογή των καταλληλότερων δημοσιεύσεων. Για το λόγο αυτό, γίνεται περαιτέρω έλεγχος ως προς τη σχετικότητα τους με το θέμα, το έτος δημοσίευσης, καθώς επίσης και ως προς τις παραπομπές, τις παραθέσεις και τον δείκτη επιστημονικής ποιότητας του κάθε άρθρου.

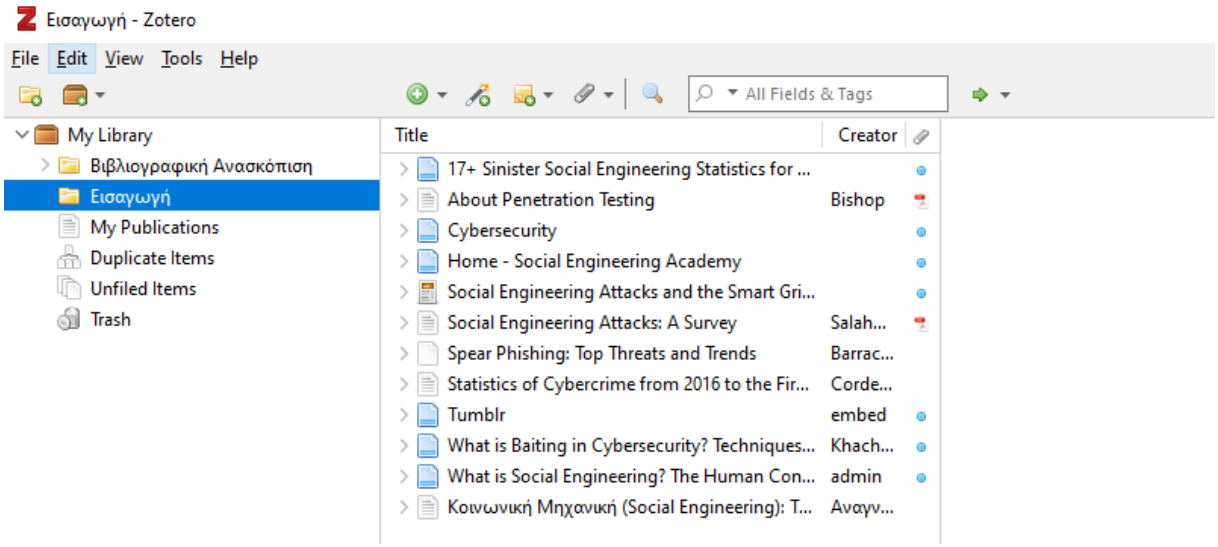
Για τη διαδικασία της αξιολόγησης και καταγραφής της βιβλιογραφίας, έγινε χρήση των λογισμικών 'Publish or Perish' και 'Zotero', με το πρώτο να χρησιμοποιείται για τον έλεγχο των

αποτελεσμάτων και το δεύτερο να χρησιμοποιείται για την καταγραφή τους, με τις σχετικές εικόνες να παρουσιάζονται πιο κάτω:



Εικόνα 3.1: Αποτελέσματα λογισμικού Publish or Perish

Στην εικόνα 5, παρουσιάζονται τα αποτελέσματα από το λογισμικό 'Publish or Perish', μετά από την αναζήτηση που έγινε με τη χρήση διαφόρων λέξεις κλειδιών. Τα αποτελέσματα είναι ταξινομημένα με αύξουσα σειρά με βάση τη στήλη 'Αναφορές' (Cites) και παρουσιάζουν πληροφορίες όπως είναι ο συγγραφέας, το έτος έκδοσης και τον οργανισμό που έκδωσε τη κάθε δημοσίευση.



Εικόνα 3.2: Λογισμικό 'Zotero'

Στην εικόνα 6, παρουσιάζεται η εφαρμογή 'Zotero', το οποίο πέρα της καταγραφής των δημοσιεύσεων, προσφέρει ταξινόμηση και αποθήκευση της βιβλιογραφίας καθώς επίσης και έναν εύκολο τρόπο αποτύπωσης της βιβλιογραφίας στην έρευνα.

Με το πέρας της έρευνας και εφόσον συγκεντρωθούν τα ανάλογα στοιχεία, μπορεί γίνει η διαδικασία επιλογής, σχεδιασμού και υλοποίησης της εκπαιδευτικής δραστηριότητας.

Η διαδικασία σχεδιασμού της δραστηριότητας, περιλαμβάνεται από μια σειρά τεσσάρων (4) σταδίων τα οποία αποτελούν:

1. Τους μαθησιακούς στόχους της δραστηριότητας,
2. Τις απαιτήσεις σχεδιασμού,
3. Τον σχεδιασμό σεναρίων
4. Την υλοποίηση της δραστηριότητας.

Στα κεφάλαια που ακολουθούν, περιγράφονται αυτά τα 4 στάδια με μια εκτενέστερη ανάλυση για το τι παραλαμβάνουν.

Κεφάλαιο 4

Σχεδιασμός Εκπαιδευτικής Δραστηριότητας

Βάση των στοιχείων της έρευνας, διαπιστώνεται ότι οι περισσότερες επιθέσεις Κοινωνικής Μηχανικής προκύπτουν μέσα από ηλεκτρονικά μηνύματα (emails) (επιθέσεις BEC), μέσω τηλεφωνικής επικοινωνίας είτε γραπτού μηνύματος (επιθέσεις Vishing και Smshing), από κακόβουλα λογισμικά (επιθέσεις Baiting και ScareWare) και από προσωπική επαφή (επιθέσεις Tailgating, Shoulder Surfing και Dumpster Diving). Για τον λόγο αυτό, κρίνεται αναγκαίο η εκπαιδευτική δραστηριότητα να επικεντρώνεται σε σενάρια για αυτού του είδους επιθέσεις.

4.1 Μαθησιακοί Στόχοι Δραστηριότητας

Παρά το γεγονός ότι οι επιτιθέμενοι δεν ορίζουν τα θύματα τους αναλόγως ηλικίας καθώς και ότι θεωρείται απαραίτητο ο κάθε ένας από εμάς να ενημερώνεται και να εκπαιδεύεται στην αντιμετώπιση των επιθέσεων Κοινωνικής Μηχανικής, εντούτοις, στην εκπαιδευτική δραστηριότητα μπορούν να λάβουν μέρος ενήλικα άτομα τα οποία εργάζονται είτε θα εργαστούν στο άμεσο μέλλον.

Με τον τρόπο αυτό, θα παρέχεται μια προετοιμασία και ενημέρωση, εξασφαλίζοντας εγρήγορση και αντίληψη για την αντιμετώπιση επιθέσεων τόσο των ιδίων όσο και των οργανισμών.

Επιπρόσθετα, οι ενήλικες, θεωρούνται περισσότερο εκτεθειμένοι σε επιθέσεις Κοινωνικής Μηχανικής, εφόσον καθημερινά γίνεται από μέρος τους η χρήση της τεχνολογίας και έχοντας επαφή με παράγοντες όπως:

- Ηλεκτρονικό ταχυδρομείο,
- Λήψη κλήσεων και μηνυμάτων στο κινητό τηλέφωνο,
- Χρήση τραπεζικών συστημάτων και λογαριασμών

- Λήψη και εγκατάσταση λογισμικών
- Πιθανή πρόσβαση σε χώρους όπου χρειάζεται εξουσιοδότηση
- Πληρωμή λογαριασμών
- Χρήση εφαρμογών κοινωνικής δικτύωσης
- Αγορά προϊόντων μέσω διαδικτύου

Στόχος της Εκπαιδευτικής Δραστηριότητας, είναι κάθε άτομο που θα λάβει μέρος, να κατανοήσει και να αναγνωρίσει τους τρόπους υλοποίησης επιθέσεων Κοινωνικής Μηχανικής, καθώς επίσης να αναπτύξει ικανότητες αντιμετώπισης αυτού του είδους επιθέσεων μέσα από εφαρμογή καλών πρακτικών. Κυριότερος στόχος όμως, είναι το κάθε άτομο που θα λάβει μέρος στη δραστηριότητα, να αντιλαμβάνεται πότε είναι θύμα και πότε εκτελείται μια επίθεσης Κοινωνικής Μηχανικής έτσι ώστε να ενεργεί για την αποτροπή των σχεδίων του επιτιθέμενου.

4.2 Απαιτήσεις Σχεδιασμού

Σε αυτή την ενότητα, παρουσιάζονται οι απαιτήσεις του σχεδιασμού, μέσα από τις οποίες καθορίζονται οι λειτουργικές απαιτήσεις καθώς επίσης και όσα αφορούν το θέμα χρηστικότητας της εκπαιδευτικής δραστηριότητας.

Η καταγραφή των απαιτήσεων του σχεδιασμού, μπορεί να γίνει σε 2 μέρη, τα οποία αποτελούν:

- Τη καταγραφή των απαιτήσεων ως προς το περιεχόμενο
- Τη καταγραφή των απαιτήσεων ως προς τη παρουσίαση

Για την περίπτωση των απαιτήσεων ως προς το περιεχόμενο, καταγράφονται τα όσα αναμένει ο χρήστης να αντικρίσει, να έχει επαφή και να μάθει μέσα από τη συγκεκριμένη εκπαιδευτική δραστηριότητα και είναι τα ακόλουθα:

- Να γίνει σωστή ενημέρωση για τους κινδύνους Κοινωνικής Μηχανικής
- Θεωρείται απαραίτητη η ενημέρωση όσον αφορά τη λήψη μέτρων για την αντιμετώπιση των επιθέσεων
- Να προσελκύσει το ενδιαφέρον όσων λάβουν μέρος τόσο ως προς το περιεχόμενο, το περιβάλλον και το στόχο της δραστηριότητας
- Η δραστηριότητα να παρουσιάζεται με τρόπο που να βοηθά τον συμμετέχοντα να κατανοεί και να απομνημονεύει αποτελεσματικά τα σημαντικά σημεία

- Να παρουσιάζεται καταγραφή αποτελεσμάτων του συμμετέχοντα για σκοπούς αξιολόγησης
- Σε κάθε περίπτωση που ο χρήστης δίνει μια απάντηση, να ενημερώνεται εάν αυτή είναι σωστή ή λανθασμένη
- Σε περίπτωση λάθος απάντησης, να παρουσιάζεται στο συμμετέχοντα επεξήγηση ή οι λόγοι που η δοθείσα απάντηση είναι λανθασμένη

Παράλληλα, στη περίπτωση των απαιτήσεων ως προς τη παρουσίαση, καταγράφονται οι τρόποι με τους οποίους η εκπαιδευτική δραστηριότητα, θα παρουσιάζεται σε ένα εύχρηστο και φιλικό περιβάλλον προς τον συμμετέχοντα, μέσα από ενέργειες όπως:

- Να υπάρχει ικανοποιητικό επίπεδο διάδρασης μεταξύ του χρήστη και της δραστηριότητας
- Το κάθε σενάριο αποτελείται από μια παράγραφο μέσα από την οποία θα αποτυπώνεται μια επίθεση Κοινωνικής Μηχανικής. Η κάθε παράγραφος πρέπει να είναι ευανάγνωστη, σύντομη περιεκτική και κατανοητή προς τον συμμετέχοντα.
- Να αποφεύγονται τεχνικές λεπτομέρειες στο βαθμό που είναι επιτρεπτό.
- Το κάθε ερώτημα και η κάθε επιλογή που θα έχει ο συμμετέχοντας να είναι κατανοητή χωρίς να δημιουργούνται ασάφειες
- Για κάθε σενάριο, θα παρουσιάζεται σχετική εικόνα για βοήθεια προς το συμμετέχοντα
- Σημαντικός παράγοντας είναι η γραμματοσειρά που θα χρησιμοποιηθεί καθώς και το χρώμα των γραμμάτων να είναι ευδιάκριτα και κατανοητά
- Προτείνεται να χρησιμοποιηθεί το μαύρο χρώμα για τα σενάρια και τις απαντήσεις
- Προτείνεται η χρήση της γραμματοσειράς 'Times New Roman'
- Η γραμματοσειρά να είναι μέγεθος 10

4.3 Σχεδιασμός Σεναρίων

Η εκπαιδευτική δραστηριότητα, υλοποιήθηκε με σκοπό την αποτελεσματική ενημέρωση σε θέματα αντιμετώπισης επιθέσεων Κοινωνικής Μηχανικής. Εστιάζεται σε διάφορα σενάρια μέσα από τα οποία περιγράφεται μια επίθεση κα ο χρήστης καλείται να επιλέξει μια απάντηση από τις τρεις (3) επιλογές που του δίνονται και οι οποίες περιγράφουν ενέργειες που θα γίνουν.

Το κάθε σενάριο είναι σε μορφή κειμένου και μαζί επισυνάπτεται εικόνα η οποία παρουσιάζει την επίθεση, με σκοπό να γίνεται κατανοητό στον χρήστη και τίθεται ένα ερώτημα στο οποίο καλείται

ο χρήστης να απαντήσει. Καθώς ο χρήστης επιλέξει μια απάντηση, παρουσιάζεται ένδειξη σε μορφή εικόνας, εάν η επιλογή του είναι ορθή ή λανθασμένη.

Σε περίπτωση που ο συμμετέχοντας επιλέξει την ορθή απάντηση, τότε συνεχίζει στο επόμενο σενάριο. Αντίθετα, σε περίπτωση επιλογής λάθος απάντησης, παρουσιάζεται επεξήγηση για το συγκεκριμένο σενάριο σε μορφή βίντεο ή κειμένου.

Σε κάθε περίπτωση, ο χρήστης μπορεί να προχωρήσει στην επόμενη επιφάνεια με την επιλογή 'Επόμενο' που βρίσκεται στο δεξί πάνω μέρος κάθε οθόνης.

Με το πέρας των ερωτήσεων και εφόσον ο χρήστης απαντήσει σε όλες, υπολογίζεται και προβάλλεται η συνολική βαθμολογία. Ο υπολογισμός, γίνεται με την πρόσθεση μιας μονάδας για κάθε σωστή απάντηση. Για κάθε λανθασμένη απάντηση δεν προστίθεται κάποιος βαθμός.

4.4 Ροή Δραστηριότητας

Στην υποενότητα αυτή, παρουσιάζεται το σχεδιάγραμμα που διαμορφώνεται μέσα από τις ερωτήσεις, τις απαντήσεις, και τις επεξηγήσεις των σεναρίων. Ακολούθως, περιγράφεται η ανάλυση που γίνεται στα σενάρια τα οποία αποτελούν τη δραστηριότητα.

4.4.1 Ανάλυση Σχεδιαγράμματος

Το σχεδιάγραμμα αποτελείται από διάφορα σχήματα με το κάθε ένα από αυτά να παρουσιάζει διαφορετικά στοιχεία. Τα σχήματα που χρησιμοποιούνται είναι τα ακόλουθα:

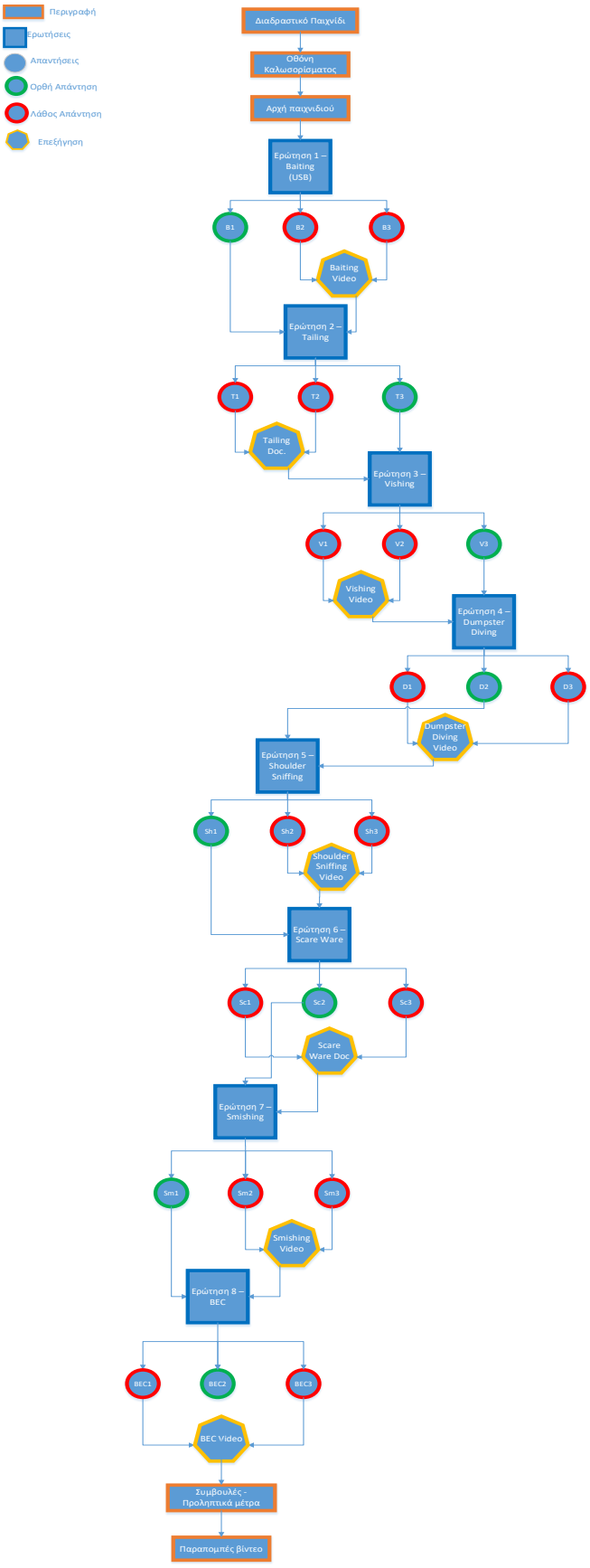
Εικόνα 4.1: Σχήματα Σχεδιαγράμματος Εκπαιδευτικής Δραστηριότητας

Το ορθογώνιο σχήμα χρησιμοποιείται για την καταχώρηση περιγραφής, ή μηνύματος που εμφανίζεται στην οθόνη του χρήστη. Το τετράγωνο σχήμα, αντιπροσωπεύει την ερώτηση που τίθεται στον χρήστη. Οι απαντήσεις των ερωτήσεων, παρουσιάζονται σε κύκλο και χωρίζονται σε 2 περιπτώσεις:

- Το κυκλικό σχήμα με πράσινο περίγραμμα αποτυπώνει την σωστή απάντηση στην ερώτηση
- Αντίθετα ο κύκλος με κόκκινο περίγραμμα, αποτυπώνει τις λανθασμένες απαντήσεις στην ερώτηση.

Επιπρόσθετα, με επτάγωνο αντιπροσωπεύει την ενημέρωση του συγκεκριμένου σεναρίου προς τον χρήστη.

Αναλυτικά το σχεδιάγραμμα παρουσιάζεται στην εικόνα 8 που παρουσιάζεται πιο κάτω:



Εικόνα 4.2: Σχεδιάγραμμα Εκπαιδευτικής Δραστηριότητας

4.4.2 Περιγραφή Ροής Δραστηριότητας

Κατά την έναρξη της εκπαιδευτικής δραστηριότητας, παρουσιάζεται σχετική εικόνα εντάσσοντας τον χρήστη στο θέμα και στο περιεχόμενο της.

Ο χρήστης με την επιλογή 'Επόμενο', συνεχίζει στην επόμενη επιφάνεια, όπου παρουσιάζεται κείμενο καλωσορίσματος και επεξήγησης του σκοπού της εκπαιδευτικής δραστηριότητας.

Ακολούθως, παρουσιάζεται εικόνα που παραπέμπει στην έναρξη της δραστηριότητας και στη συνέχεια το πρώτο από τα οχτώ (8) σενάρια που αποτελείται η δραστηριότητα.

4.4.3 Ερωτήσεις - Σενάρια

Σενάριο 1 - Baiting

Το πρώτο σενάριο αναφέρετε στην επίθεση 'Baiting'. Συγκεκριμένα, ένα εκτεθειμένο μπρελόκ με κλειδιά και USB σε χώρο στάθμευσης νοσοκομείου εντοπίζεται από νοσηλευτή ο οποίος θέλει να εντοπίσει τον ιδιοκτήτη του. Κατά την παρουσίαση του σεναρίου, προβάλλεται εικόνα με χώρο στάθμευσης νοσοκομείου. Το ερώτημα που τίθεται, είναι ποιες ενέργειες θα ακολουθήσει ο νοσηλευτής για τον εντοπισμό του ιδιοκτήτη. Στη συνέχεια ο χρήστης καλείται να επιλέξει την σωστή απάντηση η οποία σε αυτό το σενάριο είναι η πρώτη επιλογή και αναφέρεται στο να παραδώσει το μπρελόκ στο Τμήμα Πληροφορικής του νοσοκομείου. Σε περίπτωση λάθος επιλογής, προβάλλεται βίντεο μικρής διάρκειας αναφορικά με τις επιθέσεις 'Baiting' στο οποίο ο χρήστης μπορεί να περιμένει να ολοκληρωθεί για να συνεχίσει στο επόμενο σενάριο, είτε να προχωρήσει με την επιλογή 'Επόμενο'.

Σενάριο 2 - Tailgating

Ακολουθεί το δεύτερο σενάριο σχετικά με τις επιθέσεις 'Tailgating', όπου ένας ιατρός ακολουθεί τον νοσηλευτή με σκοπό να εισέλθει στο νοσοκομείο από πλαϊνή είσοδο χωρίς να έχει την απαραίτητη εξουσιοδότηση. Το ερώτημα που έχει να απαντήσει ο χρήστη είναι σε ποιες ενέργειες θα προβεί όταν διαπιστώνει ότι ακολουθείται από το άτομο αυτό.

Επιλέγοντας την τρίτη επιλογή, η οποία είναι η σωστή και αναφέρεται στο να μην του επιτρέψει την είσοδο και να τον παραπέμψει στην υποδοχή του νοσοκομείου, συνεχίζει στο επόμενο σενάριο

της δραστηριότητας. Σε αντίθετη περίπτωση, γίνεται η σχετική ενημέρωση για την επίθεση 'Tailgating' μέσω κειμένου και σχετικής εικόνας.

Σενάριο 3 - Vishing

Το τρίτο σενάριο, αναφέρεται σε επιθέσεις 'Vishing'. Σε αυτό ο νοσηλευτής βρίσκεται σε δημόσιο χώρο και δέχεται τηλεφώνημα από άτομο το οποίο του συστήνεται ως υπάλληλος τράπεζας και ζητά να γίνει επικαιροποίηση στοιχείων. Το ερώτημα του σεναρίου είναι σε ποιες ενέργειες θα προβεί ο χρήστης.

Η ορθή απάντηση για αυτό το σενάριο, είναι η τρίτη επιλογή όπου προτείνεται να προχωρήσει με την επικαιροποίηση των στοιχείων όταν δεν βρίσκεται σε δημόσιο χώρο και αφού επαληθεύσει τα στοιχεί του υπαλλήλου. Σε αντίθετα περίπτωση, ο χρήστης ενημερώνεται για τις επιθέσεις 'Vishing' μέσω βίντεο.

Σενάριο 4 - Dumpster Diving

Επόμενο σενάριο αφορά την επίθεση 'Dumpster Diving', όπου κατά τη συλλογή σκουπιδιών, εντοπίζονται σε κάδο απορριμμάτων στο γραφείο του νοσηλευτή έγγραφα με προσωπικά δεδομένα ασθενών. Το ερώτημα που τίθεται σε αυτό το σενάριο αφορά τη σωστή διαδικασία καταστροφής εγγράφων. Η ορθή απάντηση είναι η δεύτερη επιλογή όπου προτείνεται η χρήση μηχανήματος καταστροφής εγγράφων (Shredder). Σε περίπτωση που ο χρήστης επιλέξει την λάθος απάντηση, προβάλλεται βίντεο με σκοπό την ενημέρωση του χρήστη για τη συγκεκριμένη επίθεση.

Σενάριο 5 - Shoulder Surfing

Το πέμπτο σενάριο της δραστηριότητας αναφέρεται στις επιθέσεις 'Shoulder Sniffing' και σε αυτό παρουσιάζεται ο νοσηλευτής να καταχωρεί τα στοιχεία του για να εισέλθει στον ηλεκτρονικό του υπολογιστή την ώρα όμως που πίσω του βρίσκεται συνάδελφος και τον παρακολουθεί. Το ερώτημα που έχει να απαντήσει ο χρήστης αναφέρεται στο ποιες ενέργειες πρέπει να προβεί ο νοσηλευτής εφόσον αντιλαμβάνεται ότι ο συνάδελφος του κατέχει τα προσωπικά του στοιχεία. Ορθή απάντηση σε αυτή την περίπτωση να είναι η πρώτη όπου προτείνεται η άμεση αντικατάσταση των στοιχείων σε λογισμικά και υπηρεσίες όπου χρησιμοποιούνται. Σε περίπτωση λάθος απάντησης, προβάλλεται σχετικό βίντεο προς ενημέρωση.

Σενάριο 6 - Scare Ware

Επόμενη ερώτηση, είναι αναφορικά με τις επιθέσεις 'ScareWare' και το σενάριο περιγράφει την επίθεση που γίνεται μέσω ενός μηνύματος που εμφανίζεται στην επιφάνεια εργασίας του ηλεκτρονικού υπολογιστή του νοσηλευτή και τον συμβουλεύει να εγκαταστήσει συγκεκριμένο λογισμικό και να σαρώσει τον υπολογιστή του γιατί έχουν βρεθεί κακόβουλα λογισμικά σε αυτόν. Ο χρήστης καλείται να επιλέξει την ορθή απάντηση μέσα από το ερώτημα σε ποια ενέργεια πρέπει να προβεί ο νοσηλευτής, με την ορθή απάντηση να είναι η δεύτερη επιλογή όπου προτείνεται να ειδοποιηθεί το αρμόδιο τμήμα για το περιστατικό. Αν ο χρήστης επιλέξει λάθος απάντηση, ενημερώνεται για την επίθεση ScareWarte από σχετική εικόνα και κείμενο που παρουσιάζεται.

Σενάριο 7 - Smishing

Στο έβδομο σενάριο, είναι αναφορικά με τις επιθέσεις 'Smishing', όπου ο νοσηλευτής λαμβάνει μήνυμα στο κινητό του τηλέφωνο για θέματα μισθοδοσίας και καλείται να καταχωρήσει προσωπικά του στοιχεία σε συγκεκριμένη ιστοσελίδα που μπορεί να βρει μέσω συνδέσμου που επισυνάπτεται στο μήνυμα. Ο χρήστης καλείται να αποφασίσει σε ποιες ενέργειες πρέπει να προβεί ο νοσηλευτής, με την ορθή απόφαση να βρίσκεται στη δεύτερη επιλογή όπου προτείνεται να αγνοηθεί το μήνυμα. Αν ο χρήστης δεν απαντήσει σωστά, προβάλλεται βίντεο προς ενημέρωση του σχετικά με την επίθεση.

Σενάριο 8 – BEC

Στο τελευταίο σενάριο, ο νοσηλευτής, παρουσιάζεται να λαμβάνει ηλεκτρονικό μήνυμα από εξειδικευμένο ιατρό μέσα από το οποίο του ζητεί να αποσταλούν στοιχεία συγκεκριμένων ασθενών. Ο συμμετέχοντας, καλείται να απαντήσει σε ποιες ενέργειες πρέπει να προβεί ο νοσηλευτής, με την σωστή απάντηση να βρίσκεται στη δεύτερη επιλογή όπου προτείνεται να αγνοήσει το μήνυμα. Αντίθετα, σε περίπτωση που ο συμμετέχοντας επιλέξει λάθος απάντηση, προβάλλεται σύντομο βίντεο προς ενημέρωση του για τις επιθέσεις BEC.

Κεφάλαιο 5

Υλοποίηση Εκπαιδευτικής Δραστηριότητας

5.1 Αναλυτική Περιγραφή Υλοποίησης Εκπαιδευτικής Δραστηριότητας

Για την υλοποίηση της εκπαιδευτικής δραστηριότητας έγινε χρήση της πλατφόρμας 'Moodle' και του framework H5P.

Συγκεκριμένα, το Moodle αποτελεί ένα σύστημα ανοιχτού κώδικα γραμμένο σε PHP και χρησιμοποιείται για τη μικτή μάθηση, την εξ αποστάσεως εκπαίδευση, την ανατρεπόμενη τάξη και άλλα διαδικτυακά έργα μάθησης σε σχολεία, πανεπιστήμια, χώρους εργασίας και οργανισμούς.

Παράλληλα, το H5P θεωρείται πλαίσιο συνεργασίας ελεύθερου και ανοιχτού κώδικα που βασίζεται σε JavaScript και έχει ως στόχο να δημιουργεί, να μοιράζει και να επαναχρησιμοποιεί διαδραστικό περιεχόμενο μορφής HTML5 προσφέροντας τη δυνατότητα ανάπτυξης και υλοποίησης διαδραστικών βίντεο, παρουσιάσεων, κουίζ και χρονοδιαγραμμάτων.

Η εκπαιδευτική δραστηριότητα, υλοποιήθηκε με σκοπό την αποτελεσματική ενημέρωση σε θέματα αντιμετώπισης επιθέσεων Κοινωνικής Μηχανικής. Αποτελείται από 8 σενάρια και στο κάθε ένα δίνονται 3 επιλογές ως απάντηση, τις οποίες καλείται ο χρήστης να επιλέξει την ορθή.

Το κάθε ερώτημα, είναι σε μορφή κειμένου και μαζί επισυνάπτεται σχετική εικόνα για να βοηθήσει τον συμμετέχοντα να γίνει αντιληπτό το ερώτημα που τίθεται. Καθώς ο χρήστης επιλέξει μια απάντηση, παρουσιάζεται η ανάλογη εικόνα ενημερώνοντας με τον τρόπο αυτό εάν η απάντηση του είναι ορθή ή λανθασμένη.

Σε περίπτωση λάθος απάντησης, παρουσιάζεται και μια σύντομη υπόδειξη στον συμμετέχοντα αναλόγως της απάντησης που επέλεξε και ακολούθως, παρουσιάζεται μια μικρή επεξήγηση – ενημέρωση για τον τύπο της επίθεσης που αφορούσε την ερώτηση σε μορφή βίντεο ή κειμένου με σχετική εικόνα.

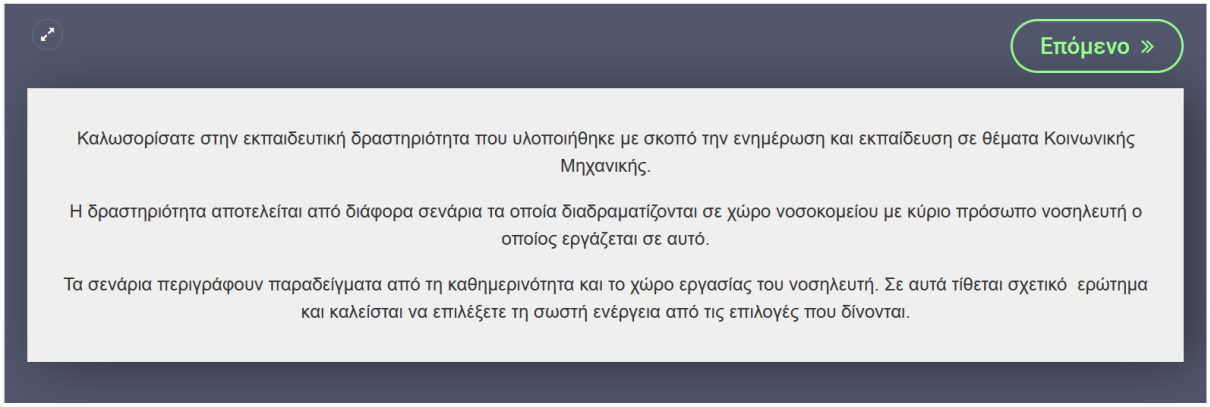
Σε κάθε περίπτωση, ο χρήστης μπορεί να προχωρήσει στην επόμενη επιφάνεια με τη επιλογή 'Επόμενο', η οποία βρίσκεται στο δεξί πάνω μέρος κάθε οθόνης.

5.2 Ροή Παιχνιδιού

Κατά την εκκίνηση του παιχνιδιού, παρουσιάζεται στον χρήστη εικόνα εντάσσοντας τον έτσι στο θέμα και στο τί θα ακολουθήσει.

Εικόνα 5.1: Εικόνα Έναρξης Εκπαιδευτικής Δραστηριότητας

Ο χρήστης με την επιλογή 'Επόμενο', συνεχίζει στην επόμενη επιφάνεια, όπου παρουσιάζεται κείμενο καλωσορίσματος και επεξήγηση για το σκοπό του εκπαιδευτικού παιχνιδιού, όπως παρουσιάζεται στην ακόλουθη εικόνα.

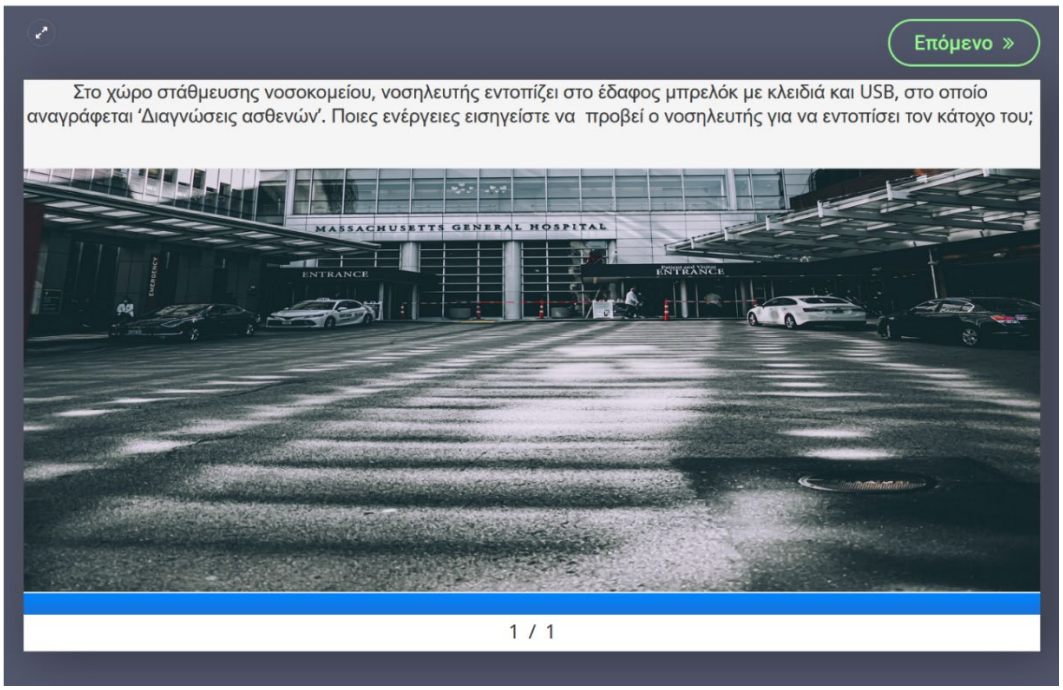


Εικόνα 5.2: Μήνυμα Καλωσορίσματος Εκπαιδευτικής Δραστηριότητας

Συνεχίζοντας, παρουσιάζεται η πιο κάτω εικόνα, η οποία παραπέμπει τον συμμετέχοντα στην έναρξη του παιχνιδιού.

Εικόνα 5.3: Εικόνα για Ενημέρωση Εκκίνησης Εκπαιδευτικής Δραστηριότητας

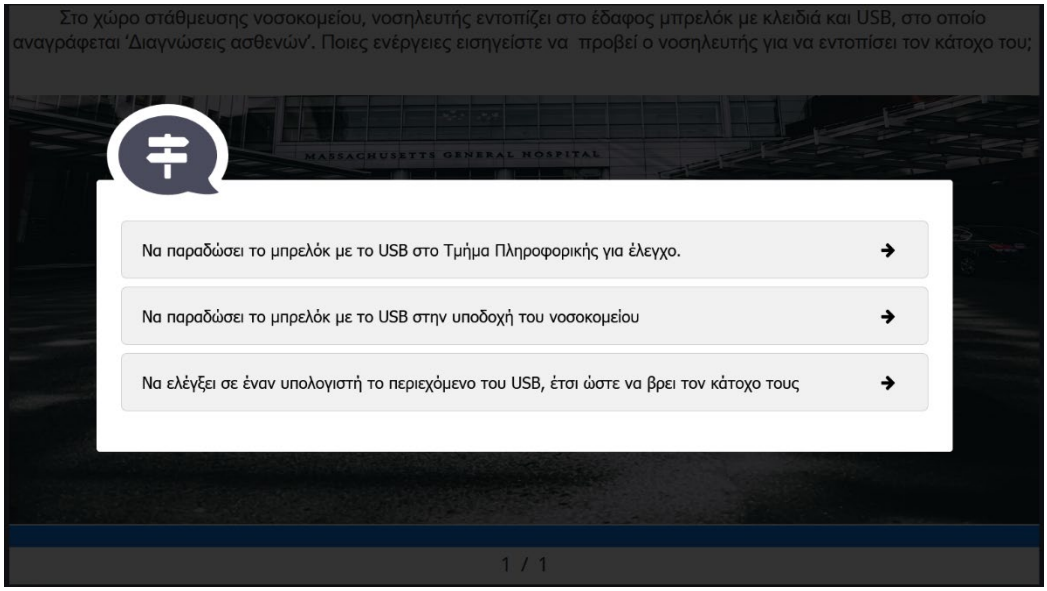
Με την έναρξη της δραστηριότητας, τίθεται η πρώτη ερώτηση η οποία αναφέρεται στις επιθέσεις μορφής Baiting. Όπως διακρίνεται στην εικόνα που ακολουθεί, το σενάριο διεξάγεται σε χώρο στάθμευσης νοσοκομείου, όπου νοσηλευτής που εργάζεται σε αυτό, εντοπίζει μπρελόκ με κλειδιά και USB στο οποίο αναγράφεται 'Διαγνώσεις Ασθενών.' Το ερώτημα που τίθεται στο εν λόγω σενάριο, είναι σε ποιες ενέργειες μπορεί να προβεί ο νοσηλευτής έτσι ώστε να βρει τον κάτοχο του USB.



Εικόνα 5.4: Σενάριο 1 - Εκπαιδευτικής Δραστηριότητας

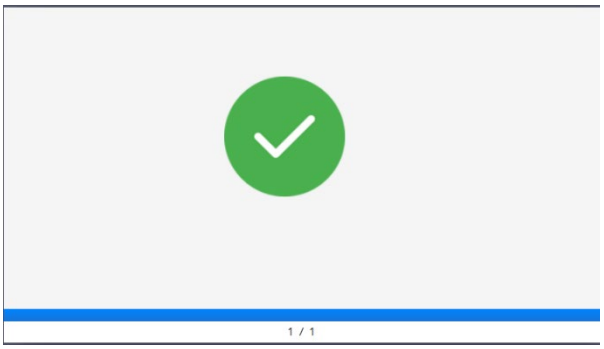
Οι επιλογές που έχει ο συμμετέχοντας, όπως φαίνεται και ακόλουθη εικόνα είναι:

1. Να παραδώσει το μπρελόκ με το USB στο Τμήμα Πληροφορικής για έλεγχο.
2. Να παραδώσει το μπρελόκ με το USB στην υποδοχή του νοσοκομείου
3. Να ελέγξει σε έναν υπολογιστή το περιεχόμενο του USB, έτσι ώστε να βρει τον κάτοχο τους



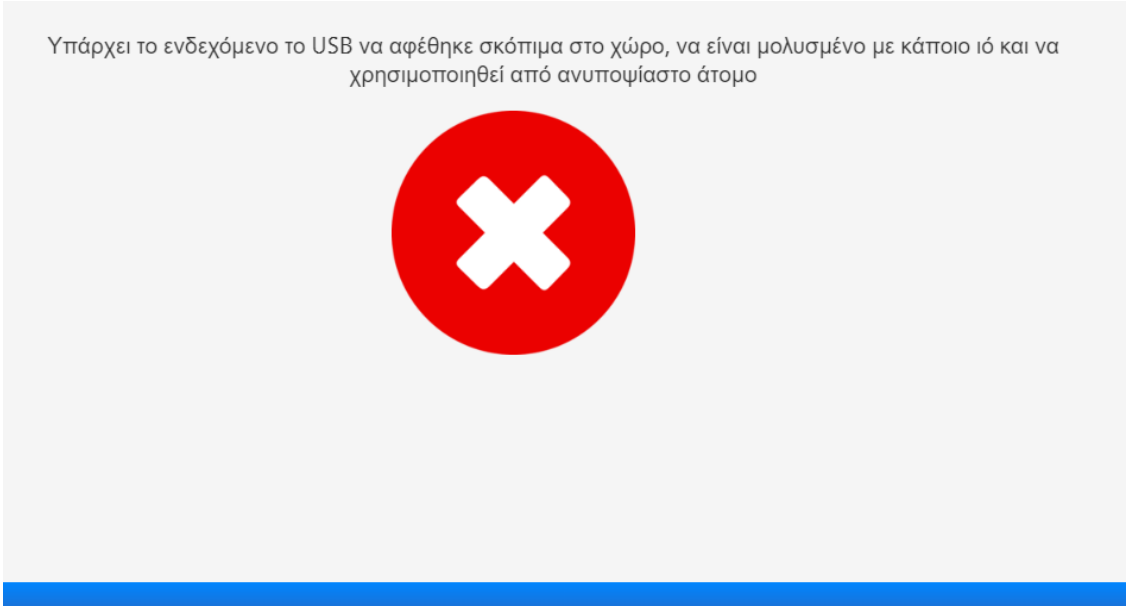
Εικόνα 5.5: Σενάριο 1 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Στη περίπτωση που ο συμμετέχοντας, επιλέξει την πρώτη επιλογή, η απάντηση του θεωρείται ορθή, οπόταν και παρουσιάζεται η πιο κάτω εικόνα



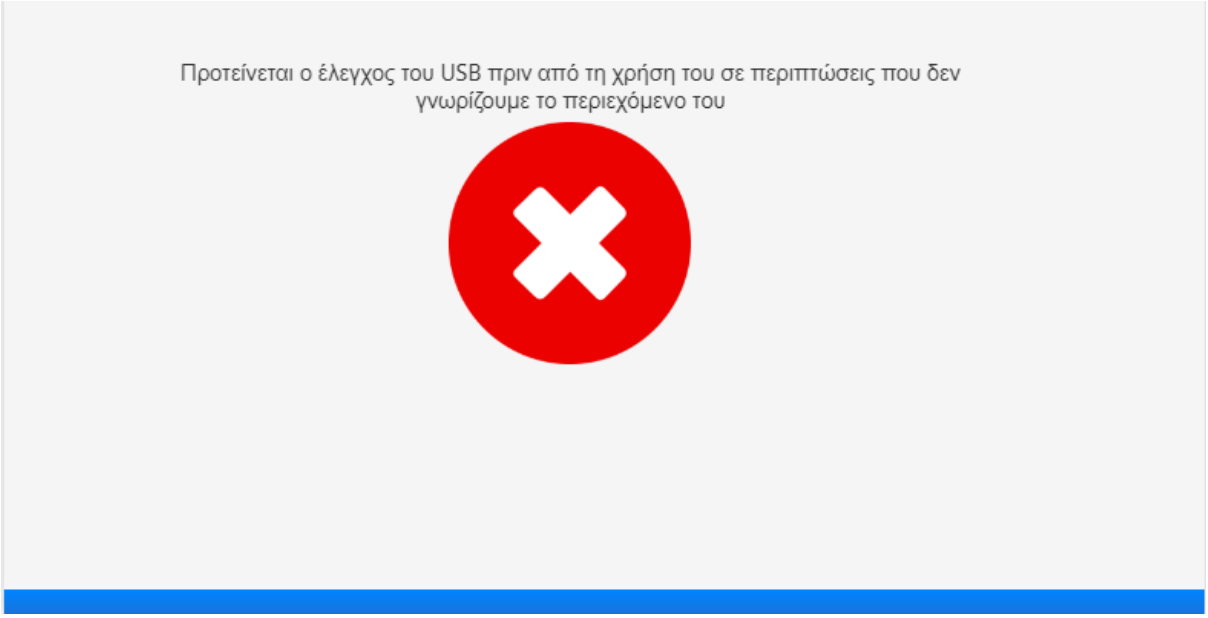
Εικόνα 5.6: Σενάριο 1 - Εικόνα Ορθής Απάντησης

Σε αντίθετη περίπτωση, εάν ο χρήστης επιλέξει τη δεύτερη επιλογή, παρουσιάζεται η εικόνα που επιδεικνύει ότι έχει επιλέξει λάθος απάντηση με μια σύντομη αναφορά σχετικά με την επιλογή του, όπου επεξηγεί στον χρήστη ότι η επιλογή του θεωρείται λανθασμένη, εφόσον με τον τρόπο αυτό, το USB μπορεί να είναι μολυσμένο και να χρησιμοποιηθεί από άτομο της υποδοχής του νοσοκομείου.



Εικόνα 5.7: Σενάριο 1 - Εικόνα Λανθασμένης Απάντησης

Όταν ο χρήστης επιλέξει την τρίτη επιλογή, παρουσιάζεται η εικόνα που τον ενημερώνει για την λάθος επιλογή του και στην οποία αναφέρεται ότι σε κάθε περίπτωση που θα γίνει χρήση USB του οποίου το περιεχόμενο δεν είναι γνωστό, προτείνεται ο έλεγχος του.

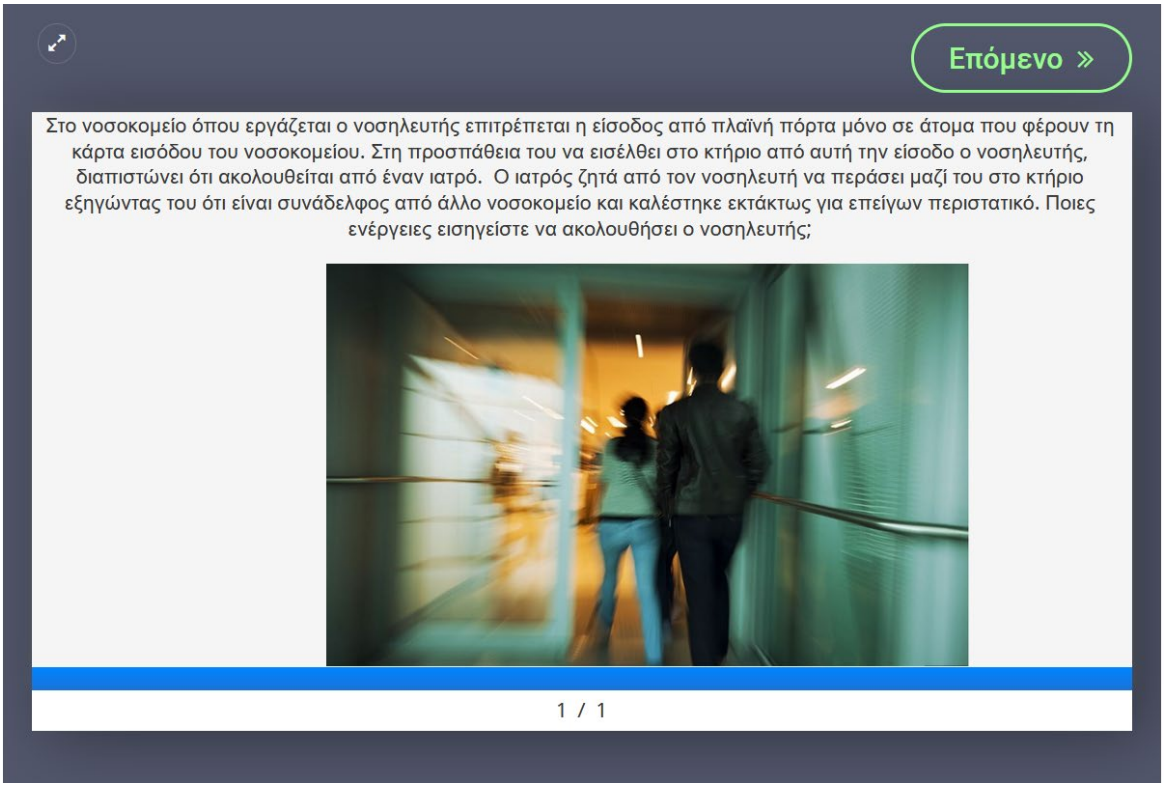


Εικόνα 5.8: Σενάριο 1 - Εικόνα Λανθασμένης Απάντησης

Μετά από την ενημέρωση του χρήστη για τη λάθος επιλογή, παρουσιάζεται ενημερωτικό βίντεο αναφορικά με την επίθεση 'Baiting' στο οποίο περιγράφεται ο τρόπος υλοποίησης της επίθεσης. Εικόνα από την έναρξη του βίντεο, παρουσιάζεται πιο κάτω:

Εικόνα 5.9: Σενάριο 1 – Ενημερωτικό Βίντεο

Με το τέλος του βίντεο, ακολουθεί η δεύτερη ερώτηση η οποία αναφέρεται στην επίθεση 'Tailgating'. Στο σενάριο αυτό όπως παρουσιάζεται και στην εικόνα που ακολουθεί, περιγράφεται ιατρός ο οποίος υποστηρίζει ότι στάλθηκε από άλλο νοσοκομείο και προσεγγίζει τον νοσηλευτή με σκοπό να του επιτραπεί η είσοδος από το πλάι με αφορμή επείγον περιστατικό, έτσι ώστε να αποφύγει τον έλεγχο της υποδοχής και τίθεται το ερώτημα σε ποιες ενέργειες εισηγείστε να ακολουθήσει ο νοσηλευτής.:



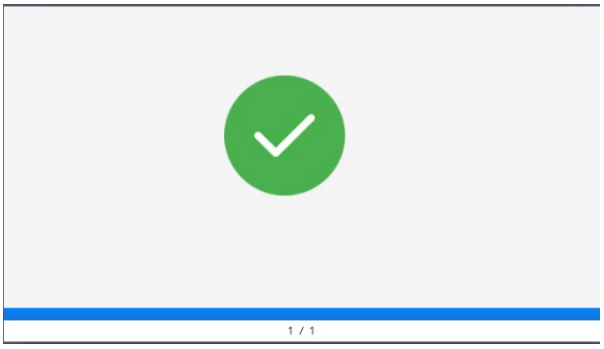
Εικόνα 5.10: Σενάριο 2 - Εκπαιδευτικής Δραστηριότητας

Οι επιλογές που προτείνονται στον χρήστη αναφορικά με την επίθεση Tailgating είναι οι ακόλουθες:

1. Να του επιτρέψει την είσοδο και να τον συνοδεύσει μέχρι το Τμήμα Επειγόντων Περιστατικών
2. Να του επιτρέψει την είσοδο και να τον παραπέμψει στην είσοδο υποδοχής για αναγνώριση ταυτότητας
3. Να μην του επιτραπεί η είσοδος και να τον παραπέμψει από την κεντρική είσοδο του κτηρίου για να περάσει από την υποδοχή του νοσοκομείου.

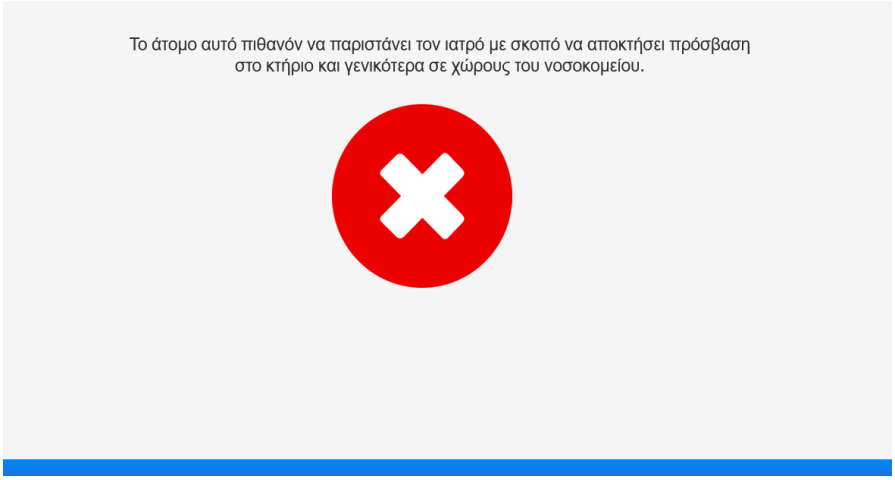
Εικόνα 5.11: Σενάριο 2 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Για το σενάριο αυτό, σωστή απάντηση είναι η τρίτη επιλογή. Επιλέγοντας την, ο χρήστης θα ενημερωθεί για την ορθή του απόφαση μέσα από την συγκεκριμένη εικόνα:



Εικόνα 5.12: Σενάριο 2 - Εικόνα Ορθής Απάντησης

Αντίθετα, αν ο χρήστης επιλέξει την πρώτη ή τη δεύτερη επιλογή, ενημερώνεται ότι η απάντηση του είναι λανθασμένη καθώς το άτομο πιθανόν να παριστάνει τον ιατρό με σκοπό να αποκτήσει πρόσβαση στο νοσοκομείο χωρίς να γίνει αντιληπτός.

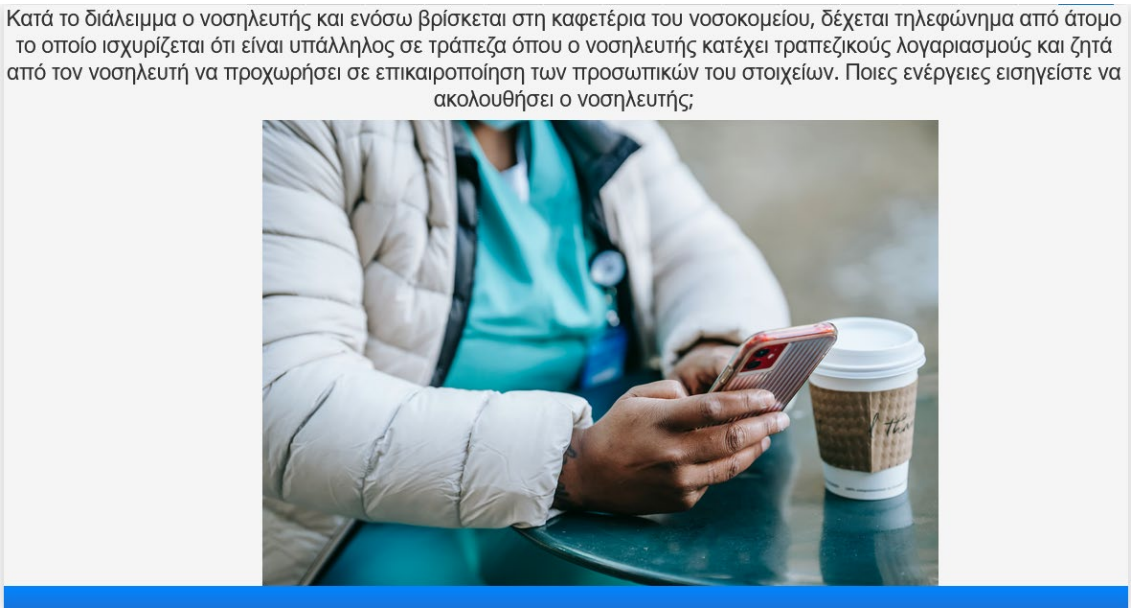


Εικόνα 5.13: Σενάριο 2 - Εικόνα Λανθασμένης Απάντησης

Ακολούθως, ο χρήστης ενημερώνεται για την επίθεση 'Tailgating' μέσω ενός κειμένου που παρουσιάζεται με σχετική εικόνα το οποίο μπορούμε να δούμε πιο κάτω:

Εικόνα 5.14: Σενάριο 2 – Ενημερωτικό Κείμενο

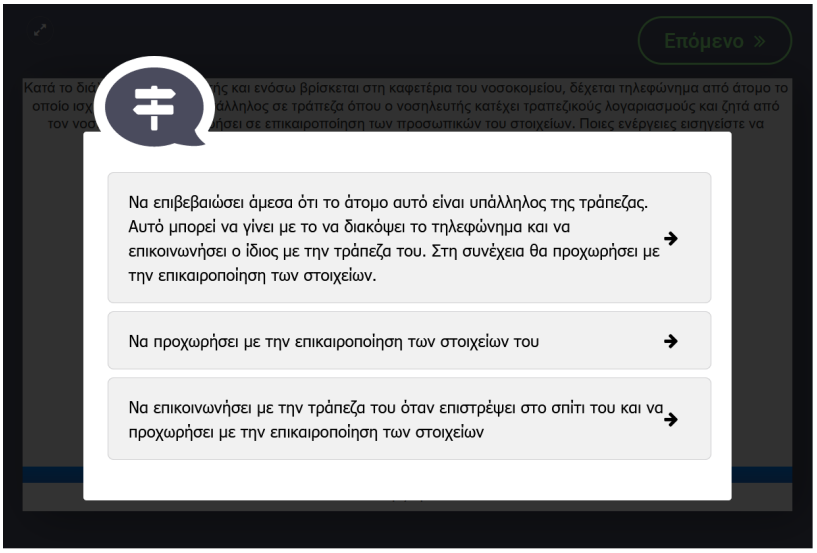
Το σενάριο που ακολουθεί αναφέρεται σε επιθέσεις 'Vishing' και σε αυτό, παρουσιάζεται ο νοσηλευτή ο οποίος βρίσκεται σε δημόσιο χώρο κατά τη διάρκεια του διαλείμματος του, να λαμβάνει τηλεφώνημα με σκοπό την επικαιροποίηση των τραπεζικών του στοιχείων. Το ερώτημα που τίθεται στον χρήστη είναι σε ποιες ενέργειες πρέπει να προβεί ο νοσηλευτής.



Εικόνα 5.15: Σενάριο 3 - Εκπαιδευτικής Δραστηριότητας

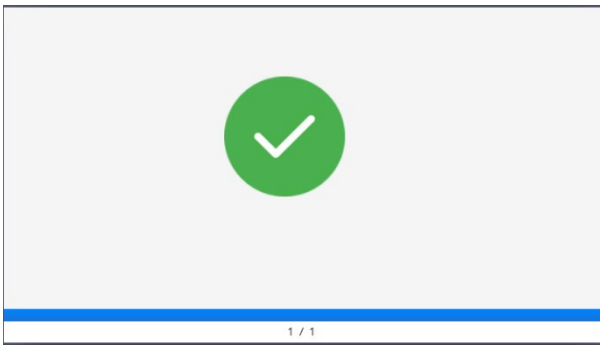
Οι επιλογές που δίνονται σε αυτό το σενάριο είναι:

1. Να επιβεβαιώσει άμεσα ότι το άτομο αυτό είναι υπάλληλος της τράπεζας. Αυτό μπορεί να γίνει με το να διακόψει το τηλεφώνημα και να επικοινωνήσει ο ίδιος με την τράπεζα του. Στη συνέχεια θα προχωρήσει με την επικαιροποίηση των στοιχείων.
2. Να προχωρήσει με την επικαιροποίηση των στοιχείων του
3. Να επικοινωνήσει με την τράπεζα του όταν επιστρέψει στο σπίτι του και να προχωρήσει με την επικαιροποίηση των στοιχείων



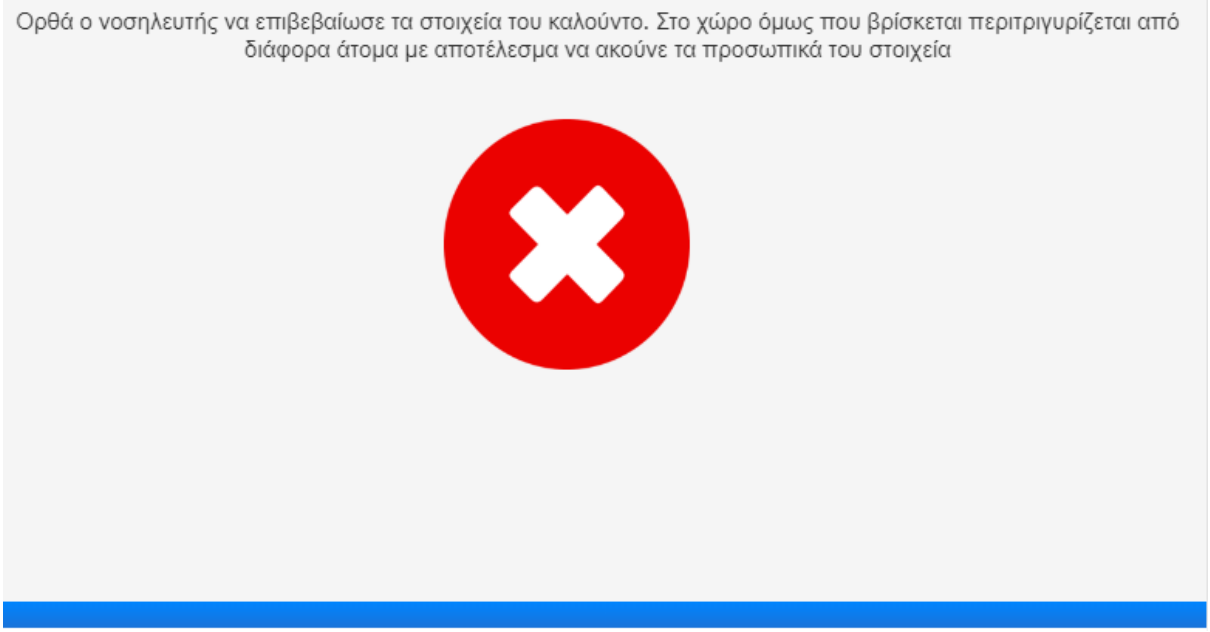
Εικόνα 5.16: Σενάριο 3 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Επιλέγοντας την τρίτη επιλογή η οποία είναι και η σωστή, θα ενημερωθεί ο χρήστης για την ορθή απάντηση του με την αντίστοιχη εικόνα:



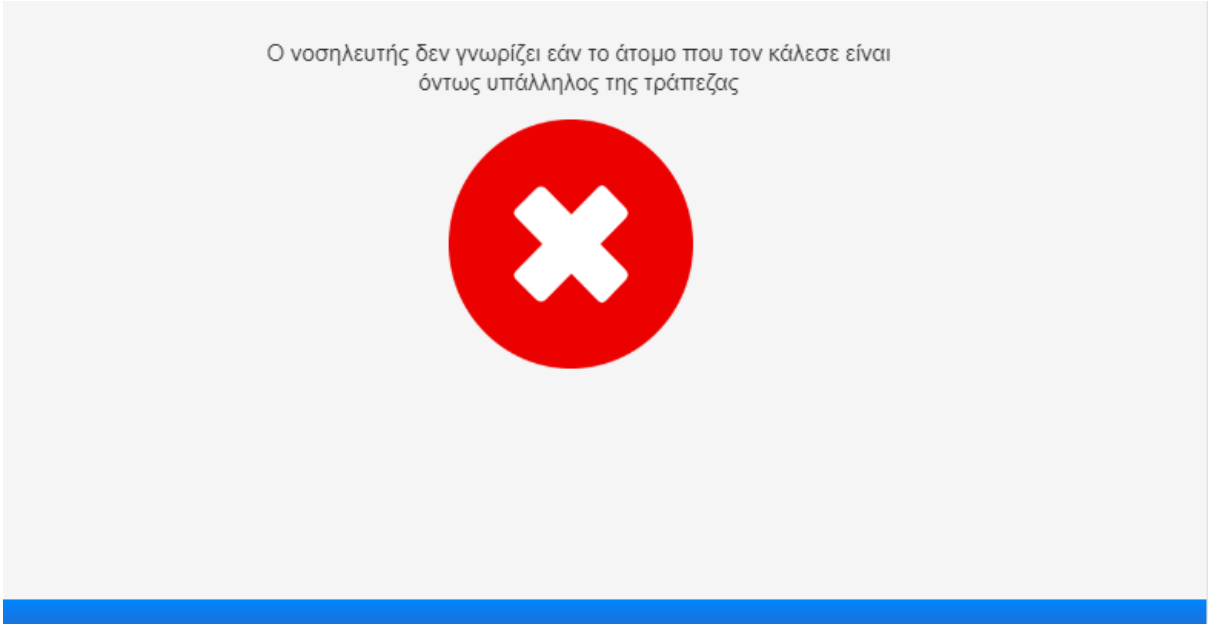
Εικόνα 5.17: Σενάριο 3 - Εικόνα Ορθής Απάντησης

Αντίθετα, σε περίπτωση που ο συμμετέχοντας επιλέξει την πρώτη επιλογή, ενημερώνεται ότι μπορεί ο νοσηλευτής να επιβεβαίωσε τα στοιχεί του ατόμου που τον καλεί, όμως, στον χώρο όπου βρίσκεται και προβαίνει σε επικαιροποίηση των στοιχείων βρίσκονται διάφορα άτομα με αποτέλεσμα να μπορούν να ακούνε τη συνομιλία του και τα προσωπικά στοιχεία που δίνει.



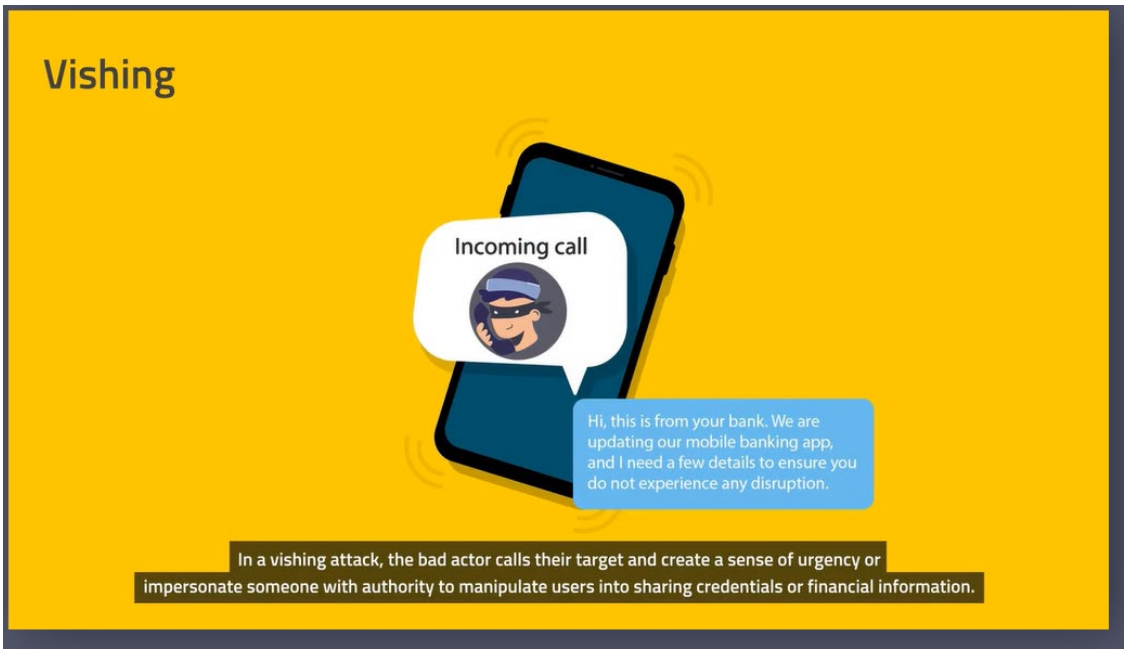
Εικόνα 5.18: Σενάριο 3 - Εικόνα Λανθασμένης Απάντησης

Λάθος απάντηση θεωρείται και η δεύτερη επιλογή, εφόσον ο νοσηλευτής δεν προέβει σε κάποια ενέργεια για εξακρίβωση των στοιχείων του ατόμου που τον καλεί.



Εικόνα 5.19: Σενάριο 3 - Εικόνα Λανθασμένης Απάντησης

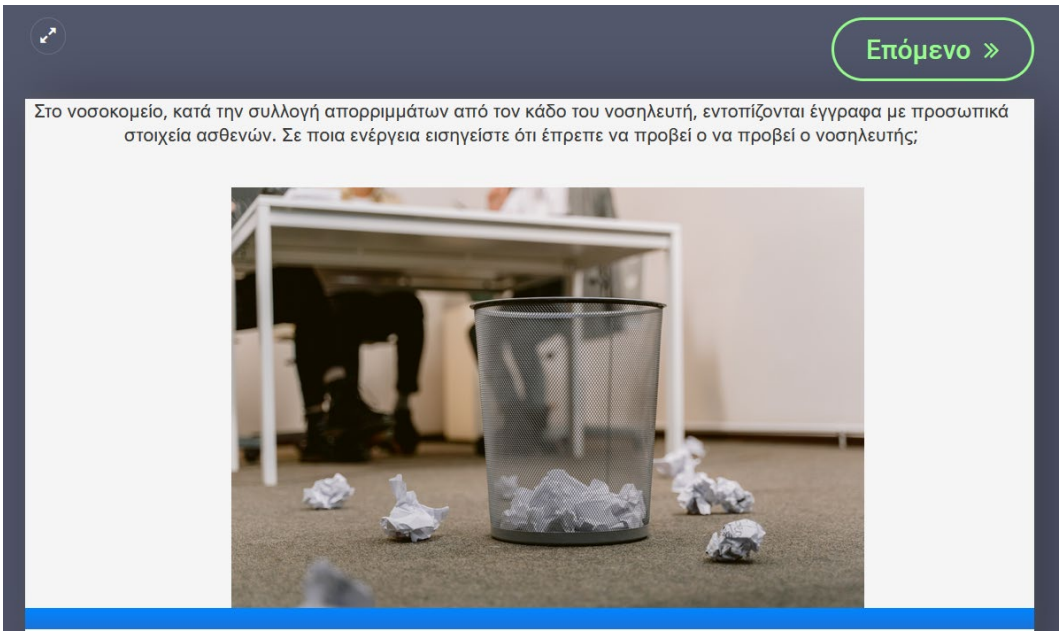
Για ενημέρωση του συμμετέχοντα σχετικά με τις επιθέσεις 'Vishing', προβάλλεται μικρής διάρκειας βίντεο σχετικά με την επίθεση.



Εικόνα 5.20: Σενάριο 3 – Ενημερωτικό Βίντεο

Το επόμενο σενάριο, αναφέρετε σε επιθέσεις 'Dumpster Diving' και σε αυτό περιγράφεται ότι κατά τη διαδικασία συλλογής απορριμμάτων από τον κάδο του

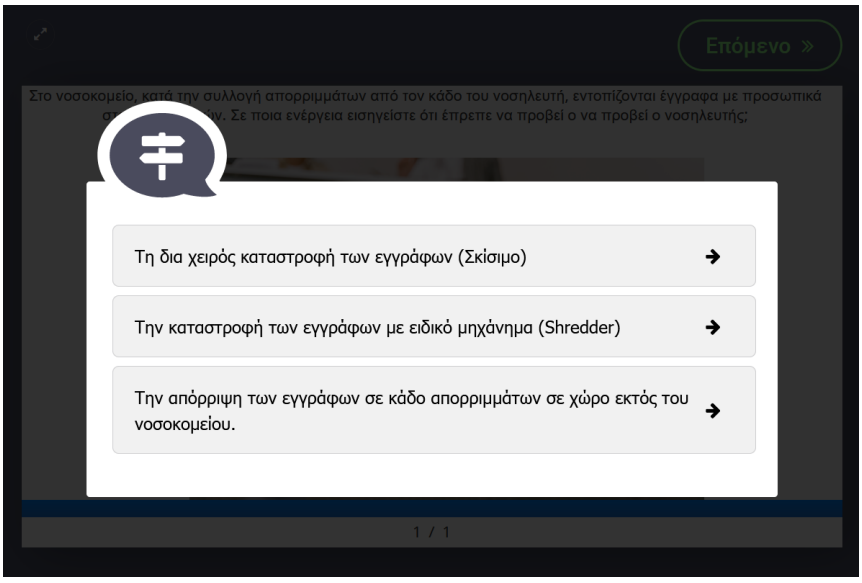
νοσηλευτή, εντοπίζονται έγγραφα με προσωπικά στοιχεία ασθενών. Η ερώτηση που έχει να απαντήσει ο χρήστης είναι σε ποιες ενέργειες έπρεπε να προβεί ο νοσηλευτής.



Εικόνα 5.21: Σενάριο 4 - Εκπαιδευτικής Δραστηριότητας

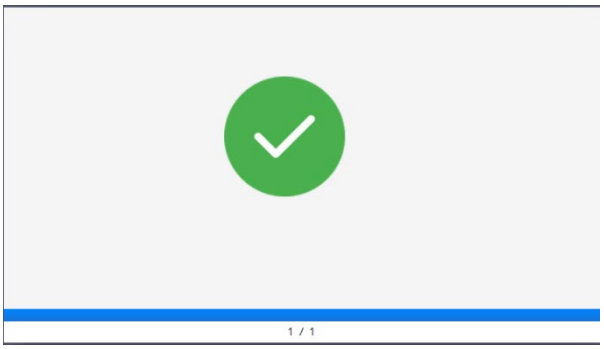
Οι επιλογές που προτείνονται είναι:

1. Τη δια χειρός καταστροφή των εγγράφων (Σκίσιμο)
2. Την καταστροφή των εγγράφων με ειδικό μηχάνημα (Shredder),
3. Την απόρριψη των εγγράφων σε κάδο απορριμμάτων σε χώρο εκτός του νοσοκομείου.



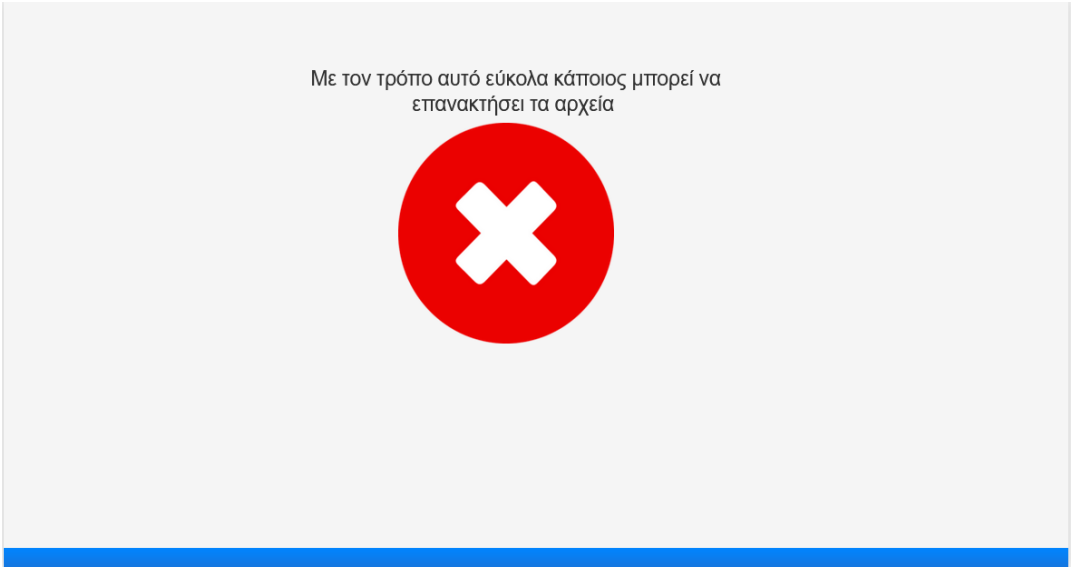
Εικόνα 5.22: Σενάριο 4 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Ορθή απάντηση αυτού του σεναρίου, είναι η δεύτερη επιλογή όπου προτείνεται η καταστροφή των εγγράφων με τη χρήση ειδικού μηχανήματος. Επιλέγοντας την ο χρήστης ενημερώνεται ότι η απάντηση είναι σωστή με τη σχετική εικόνα.



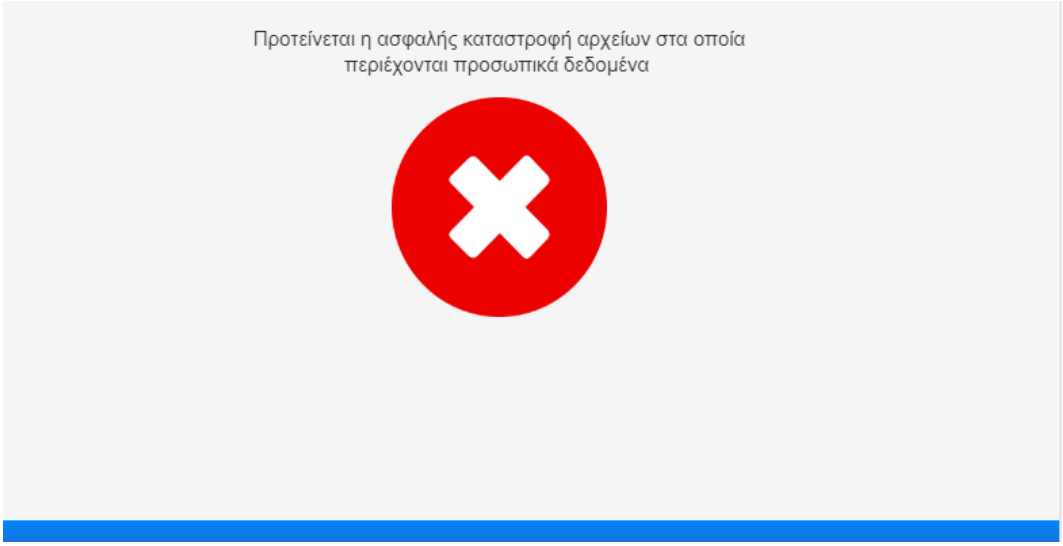
Εικόνα 5.23: Σενάριο 4 - Εικόνα Ορθής Απάντησης

Σε περίπτωση που ο χρήστης επιλέξει την πρώτη επιλογή, η οποία είναι λανθασμένη, ενημερώνεται μέσω σχετικής εικόνας, στην οποία αναφέρεται ότι με τον τρόπο αυτό, εύκολα κάποιος μπορεί να ανακτήσει τα αρχεία.



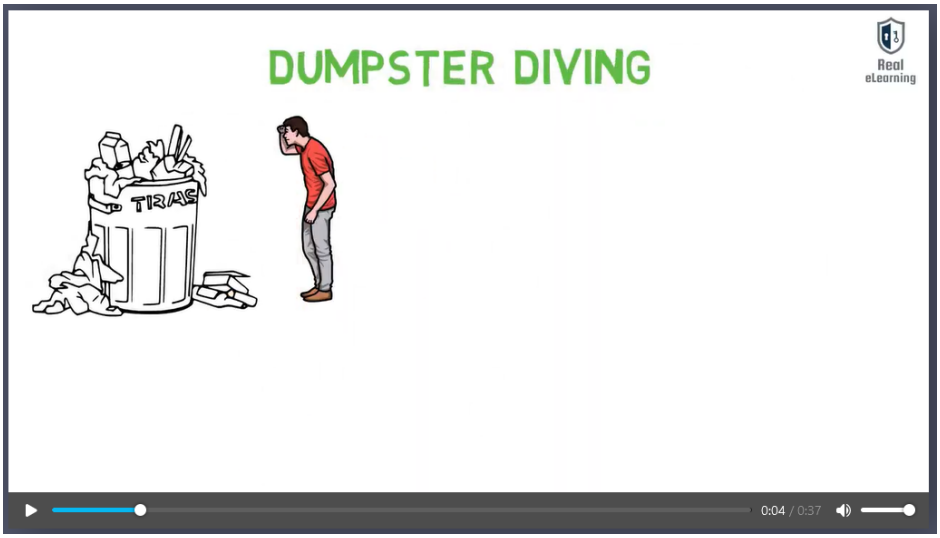
Εικόνα 5.24: Σενάριο 4 - Εικόνα Λανθασμένης Απάντησης

Με την τρίτη επιλογή η οποία είναι εξίσου λανθασμένη, ο χρήστης ενημερώνεται ότι σε αρχεία όπου περιέχονται προσωπικά στοιχεία, πρέπει να καταστρέφονται έτσι ώστε η ανάκτηση τους να είναι αδύνατη.



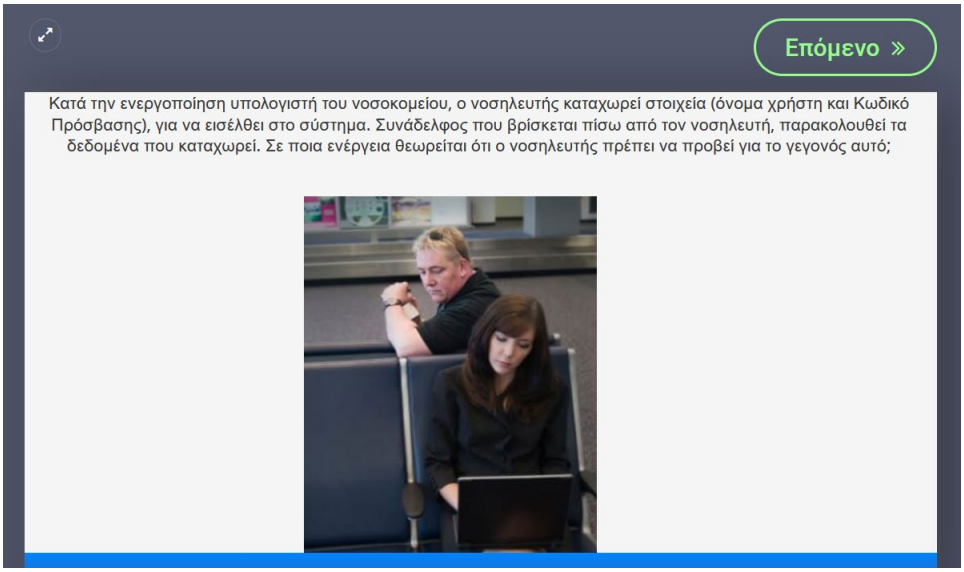
Εικόνα 5.25: Σενάριο 4 - Εικόνα Λανθασμένης Απάντησης

Στη συνέχεια προβάλλεται βίντεο σχετικά με την επίθεση ‘Dumpster Diving’ με σκοπό την περεταίρω ενημέρωση του χρήστη.



Εικόνα 5.26: Σενάριο 4 – Ενημερωτικό Βίντεο

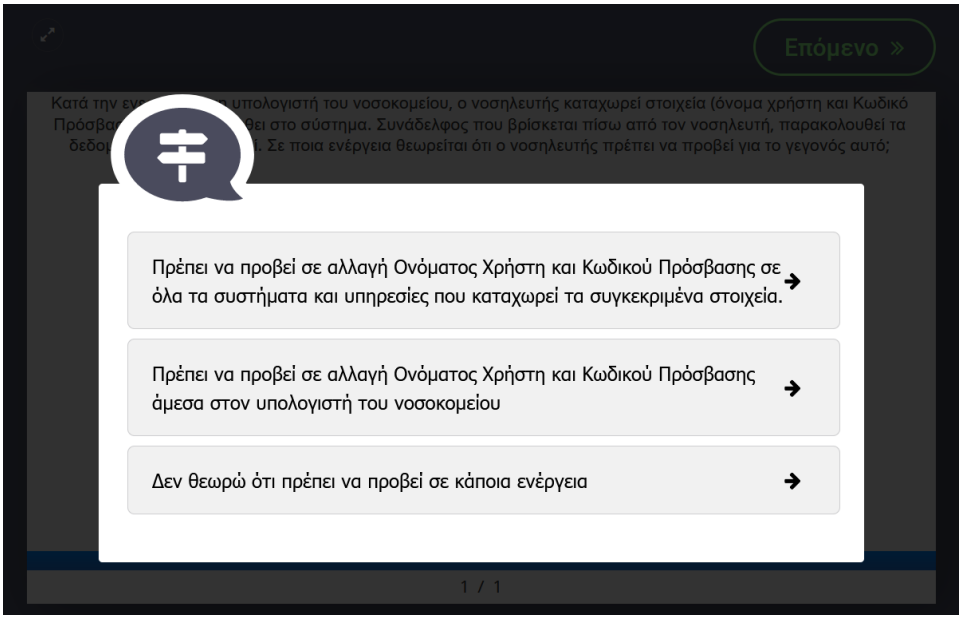
Το επόμενο σενάριο, αναφέρεται στις επιθέσεις ‘Shoulder Sniffing’. Σε αυτό παρουσιάζεται ο νοσηλευτής να εισάγει τα διαπιστευτήρια του στον ηλεκτρονικό υπολογιστή για να εισέλθει στο σύστημα του νοσοκομείου την ώρα όμως που συνάδελφος του βρίσκεται πίσω του και παρακολουθεί τα στοιχεία που καταχωρεί. Το ερώτημα που έχει να απαντήσει ο χρήστης, είναι σε ποια ενέργεια πρέπει να προβεί ο νοσηλευτής, αφού αντιλαμβάνεται το γεγονός αυτό.



Εικόνα 5.27: Σενάριο 5 - Εκπαιδευτικής Δραστηριότητας

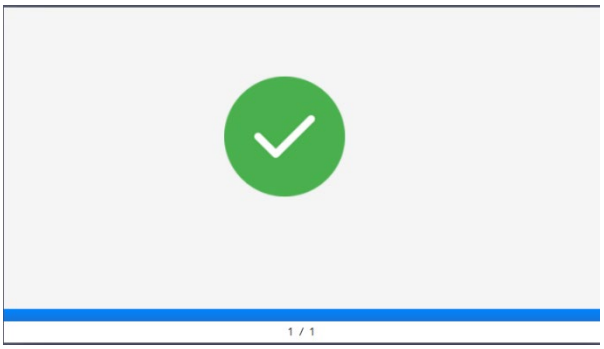
Για την ερώτηση αυτή, οι απαντήσεις που έχει ο χρήστης στη διάθεση του είναι οι ακόλουθες:

1. Πρέπει να προβεί σε αλλαγή Ονόματος Χρήστη και Κωδικού Πρόσβασης σε όλα τα συστήματα και υπηρεσίες που καταχωρεί τα συγκεκριμένα στοιχεία.
2. Πρέπει να προβεί σε αλλαγή Ονόματος Χρήστη και Κωδικού Πρόσβασης άμεσα στον υπολογιστή του νοσοκομείου
3. Δεν θεωρώ ότι πρέπει να προβεί σε κάποια ενέργεια



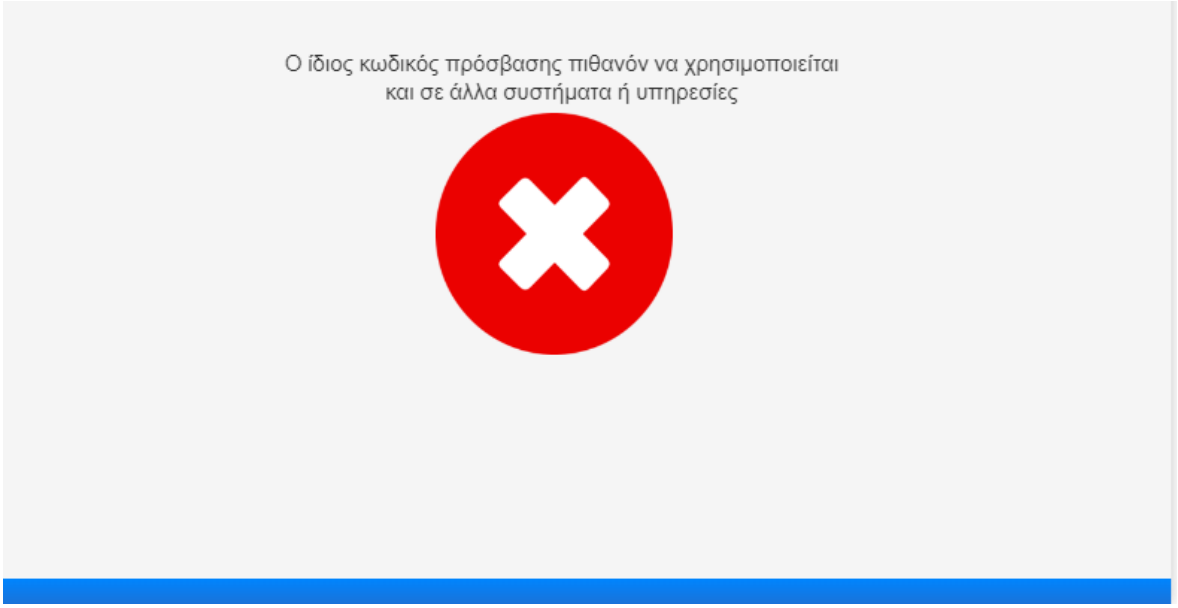
Εικόνα 5.28: Σενάριο 5 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Στο σενάριο αυτό ορθή απάντηση θεωρείται η πρώτη επιλογή, όπου προτείνεται η αλλαγή σε όλα τα συστήματα και υπηρεσίες που χρησιμοποιεί τα ίδια διαπιστευτήρια.



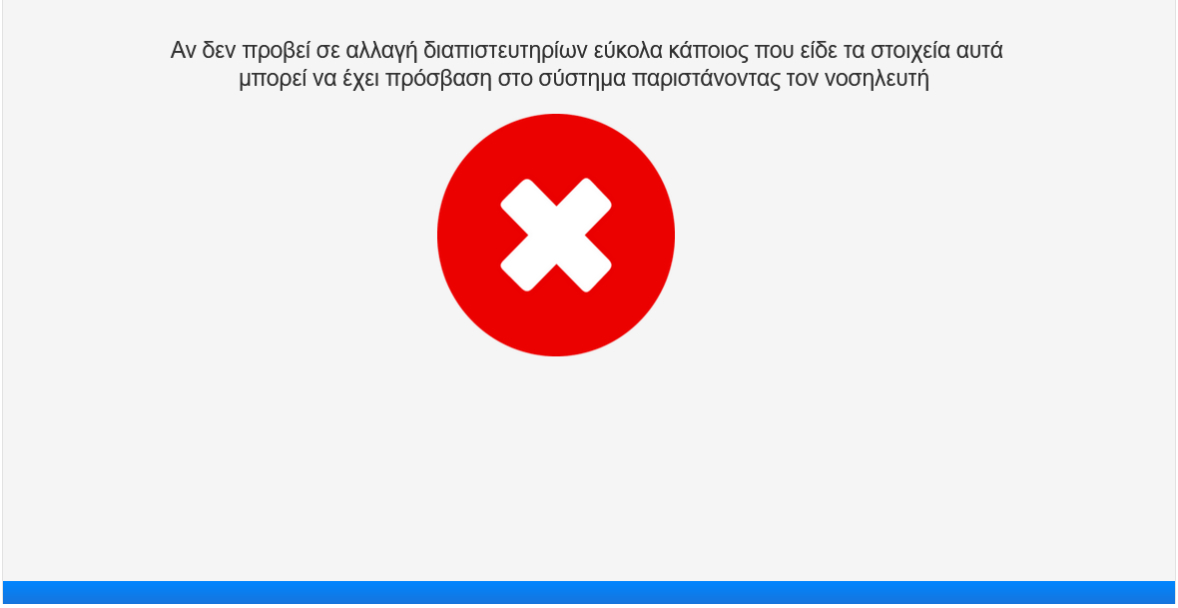
Εικόνα 5.29: Σενάριο 5 - Εικόνα Ορθής Απάντησης

Σε αντίθετη περίπτωση, επιλέγοντας τη δεύτερη επιλογή, ο χρήστης ενημερώνεται για τη λάθος απόφαση του με τη σχετική εικόνα, στην οποία ενημερώνει τον χρήστη ότι ο ίδιος κωδικός πρόσβασης μπορεί να χρησιμοποιείται σε διάφορα συστήματα ή υπηρεσίες.



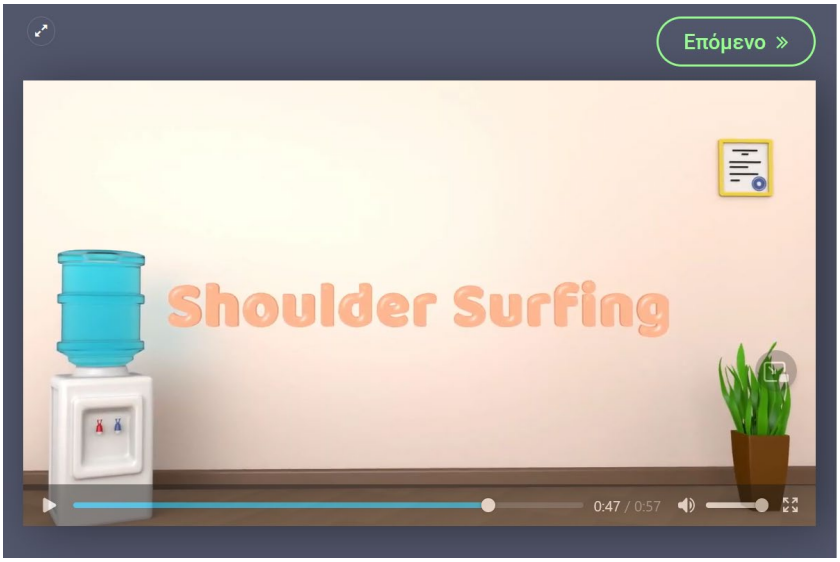
Εικόνα 5.30: Σενάριο 5 - Εικόνα Λανθασμένης Απάντησης

Αν χρήστης επιλέξει την τρίτη επιλογή η οποία είναι λανθασμένη, ενημερώνεται μέσω της σχετικής εικόνας στην οποία επεξηγεί ότι αν δεν γίνει αλλαγή των στοιχείων υπάρχει κίνδυνος πρόσβασης στο σύστημα από 3ο άτομο.



Εικόνα 5.31: Σενάριο 5 - Εικόνα Λανθασμένης Απάντησης

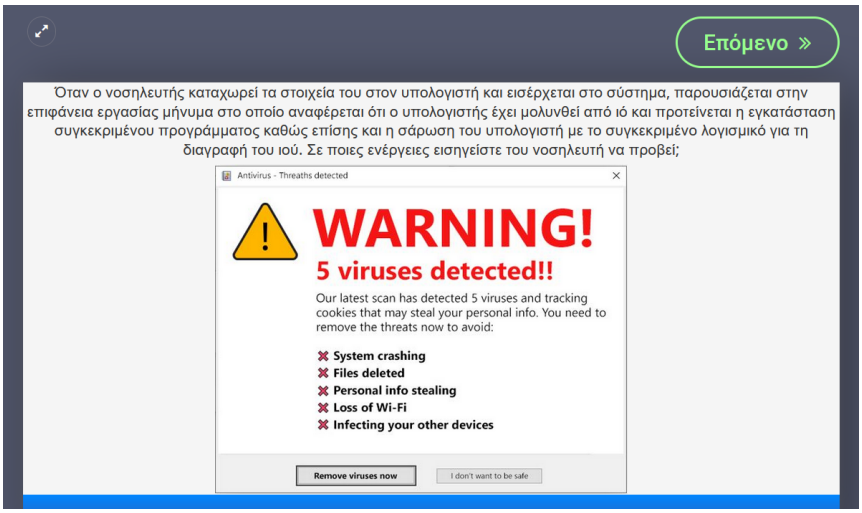
Στη συνέχεια προβάλλεται σχετικό βίντεο το οποίο παρουσιάζει τις επιθέσεις μορφής Shoulder Surfing.



Εικόνα 5.32: Σενάριο 5 – Ενημερωτικό Βίντεο

Μετά από την επίθεση 'Shoulder Surfing', προβάλλεται το σενάριο σχετικά με τις επιθέσεις 'Scare Ware', όπου ο νοσηλευτής όταν εισέρχεται στο σύστημα έρχεται αντιμέτωπος με ένα απρόσμενο μήνυμα μέσα από το οποίο ενημερώνεται ότι ο υπολογιστής έχει επιρεαστεί από ιό και προτείνεται η εγκατάσταση συγκεκριμένου λογισμικού καθώς επίσης και η σάρωση του με το εν λόγω λογισμικό για την επίλυση η

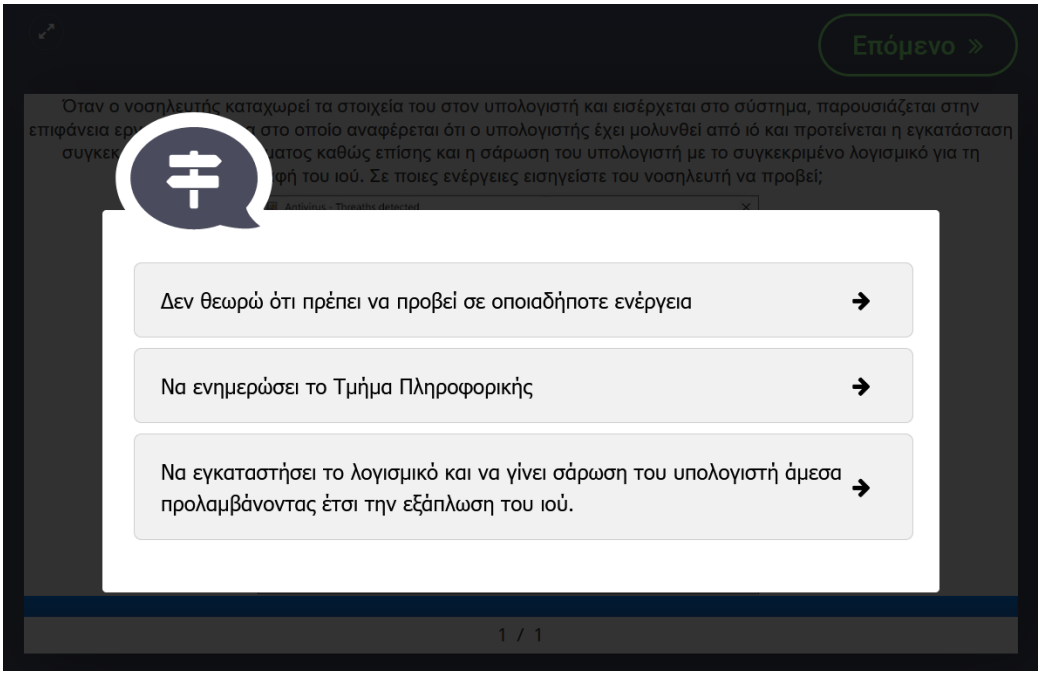
του προβλήματος. Το ερώτημα που έχει να απαντήσει ο συμμετέχοντας, είναι σε ποιες ενέργειες πρέπει να προβεί ο νοσηλευτής.



Εικόνα 5.33: Σενάριο 6 - Εκπαιδευτικής Δραστηριότητας

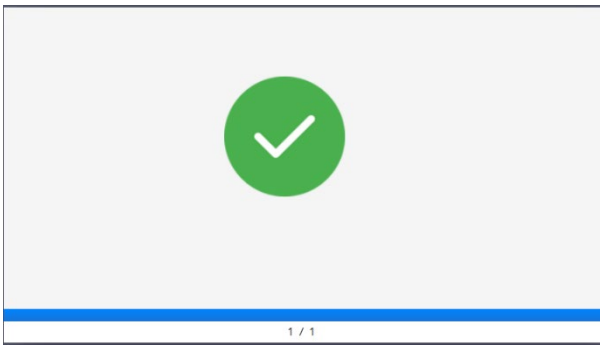
Οι ενέργειες που προτείνονται είναι οι ακόλουθες:

1. Δεν θεωρώ ότι πρέπει να προβεί σε οποιαδήποτε ενέργεια
2. Να ενημερώσει το Τμήμα Πληροφορικής
3. Να εγκαταστήσει το λογισμικό και να γίνει σάρωση του υπολογιστή άμεσα προλαμβάνοντας έτσι την εξάπλωση του ιού.



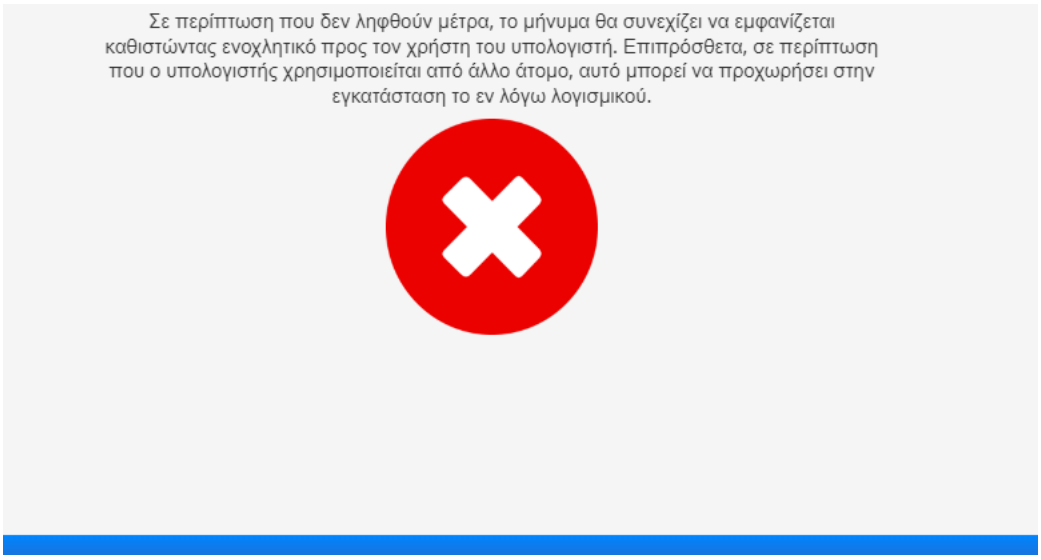
Εικόνα 5.34: Σενάριο 6 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Ορθή επιλογή για του σεναρίου, είναι η δεύτερη μέσα από την οποία προτείνεται η ενημέρωση του Τμήματος Πληροφορικής. Επιλέγοντας την ο χρήστης ενημερώνεται για την ορθή του απόφαση μέσω της σχετικής εικόνας:



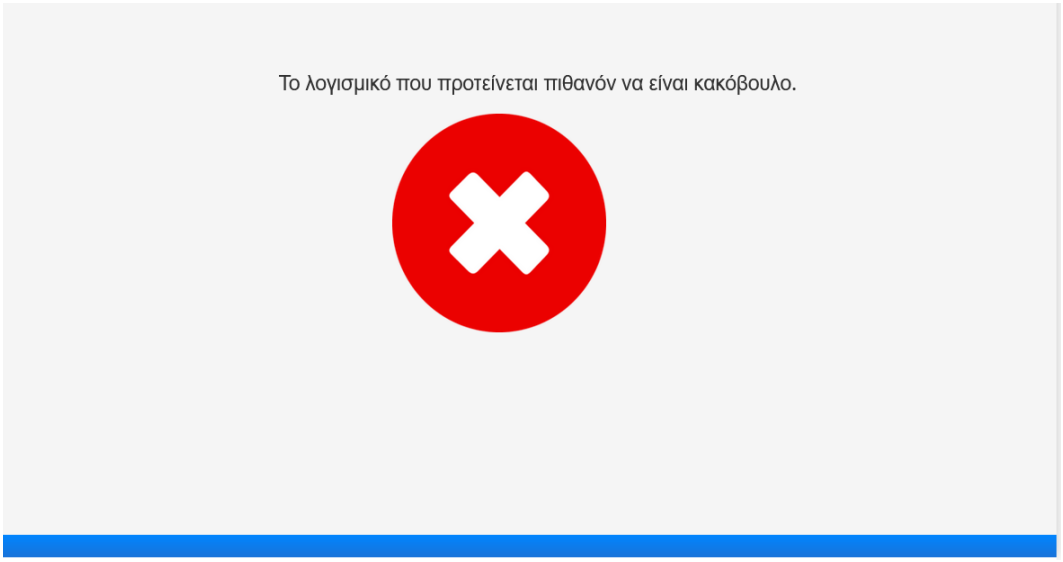
Εικόνα 5.35: Σενάριο 6 - Εικόνα Ορθής Απάντησης

Σε αντίθετη περίπτωση αν ο συμμετέχοντας επιλέξει την πρώτη απάντηση, τότε ενημερώνεται για το λάθος, καθώς επίσης ότι υπάρχει ενδεχόμενο πρόκλησης μεγαλύτερης ζημιάς αν δεν ληφθούν τα απαραίτητα μέτρα.



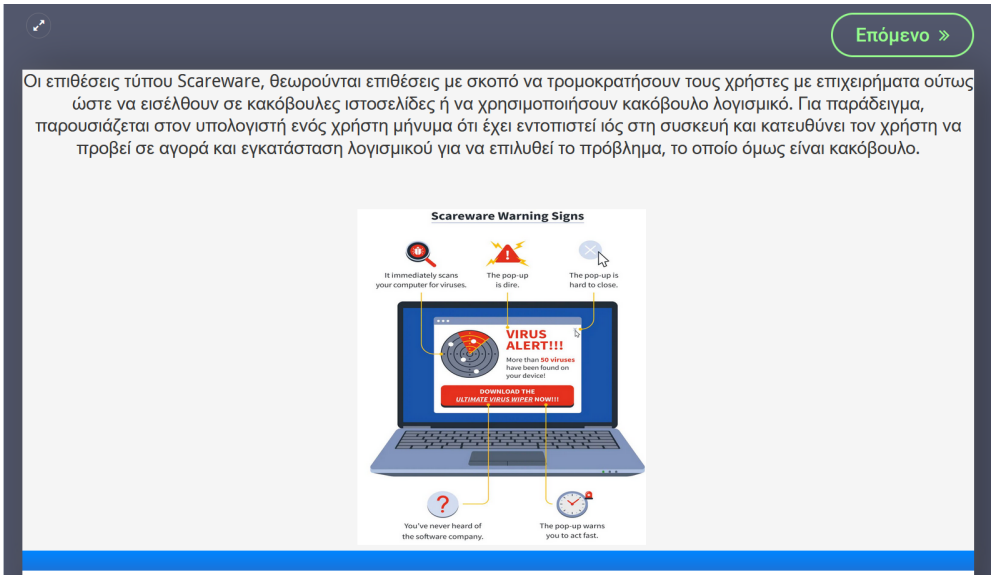
Εικόνα 5.36: Σενάριο 6 - Εικόνα Λανθασμένης Απάντησης

Λανθασμένη απάντηση θεωρείται και η τρίτη επιλογή. Σε περίπτωση επιλογής της, ο χρήστης ενημερώνεται για το λάθος του μέσω της σχετικής εικόνας και της επεξήγησης ότι το λογισμικό που προτείνεται να εγκατασταθεί, πιθανόν να είναι κακόβουλο.



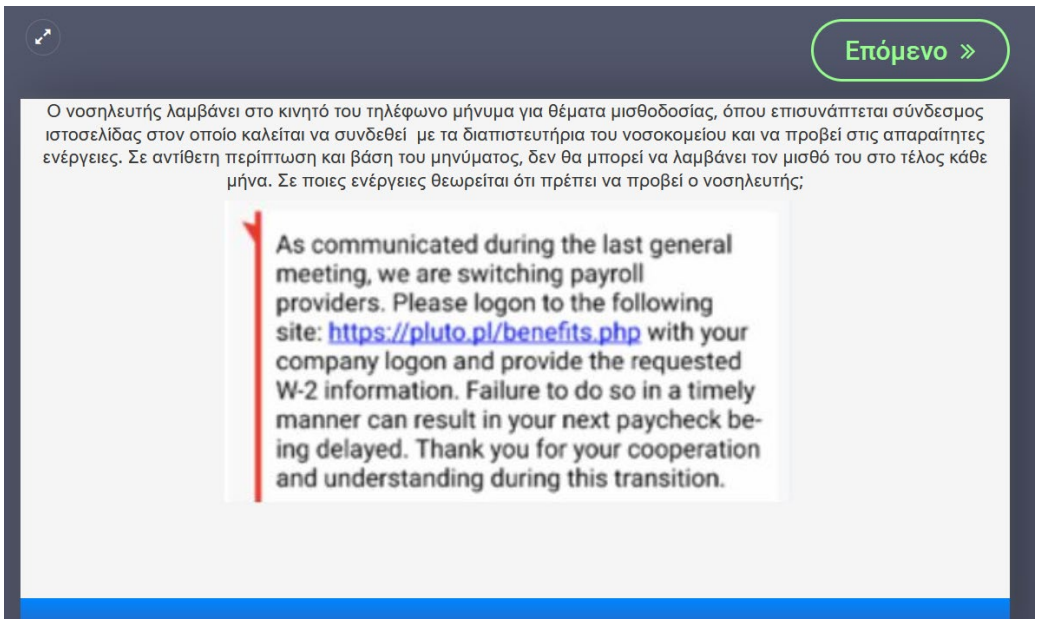
Εικόνα 5.37: Σενάριο 6 - Εικόνα Λανθασμένης Απάντησης

Ακολούθως, προβάλλεται στον συμμετέχοντα εικόνα με ενημερωτικό κείμενο αναφορικά με τις επιθέσεις μορφής Scare Ware, η οποία παρουσιάζεται στην εικόνα 5.38



Εικόνα 5.38: Σενάριο 6 - Ενημερωτικό Βίντεο

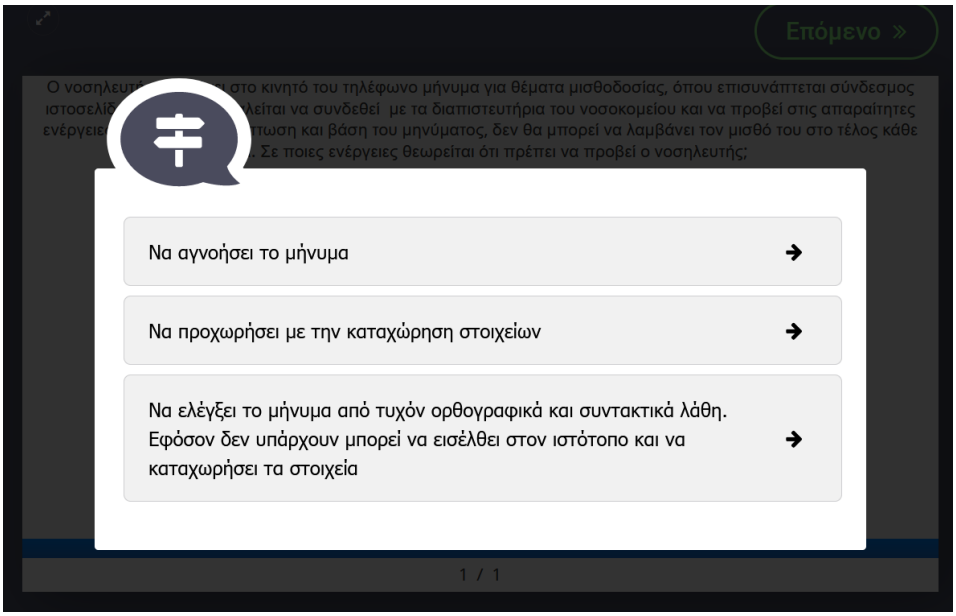
Στο έβδομο σενάριο, παρουσιάζεται ο νοσηλευτής να λαμβάνει μήνυμα στο κινητό του τηλέφωνό, για θέματα μισθοδοσίας και στο οποίο επισυνάπτεται σύνδεσμος όπου καλείται να συνδεθεί για να προβεί στις απαραίτητες ενέργειες. Σύμφωνα με το μήνυμα, σε αντίθετη περίπτωση ο νοσηλευτής δεν θα είναι σε θέση να λαμβάνει τον μισθό του κάθε τέλος του μήνα.



Εικόνα 5.39: Σενάριο 7 - Εκπαιδευτικής Δραστηριότητας

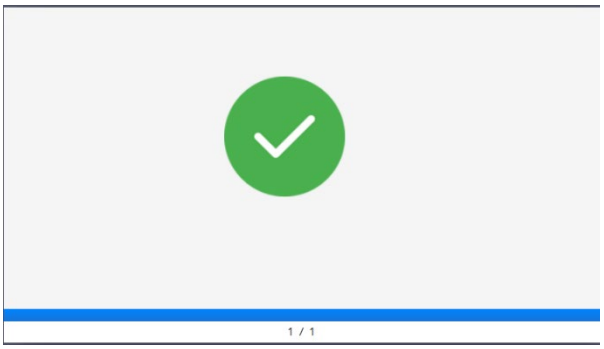
Για το σενάριο αυτό προτείνονται οι ακόλουθες ενέργειες:

1. Να αγνοήσει το μήνυμα
2. Να προχωρήσει με την καταχώρηση στοιχείων
3. Να ελέγξει το μήνυμα από τυχόν ορθογραφικά και συντακτικά λάθη. Εφόσον δεν υπάρχουν μπορεί να εισέλθει στον ιστότοπο και να καταχωρήσει τα στοιχεία



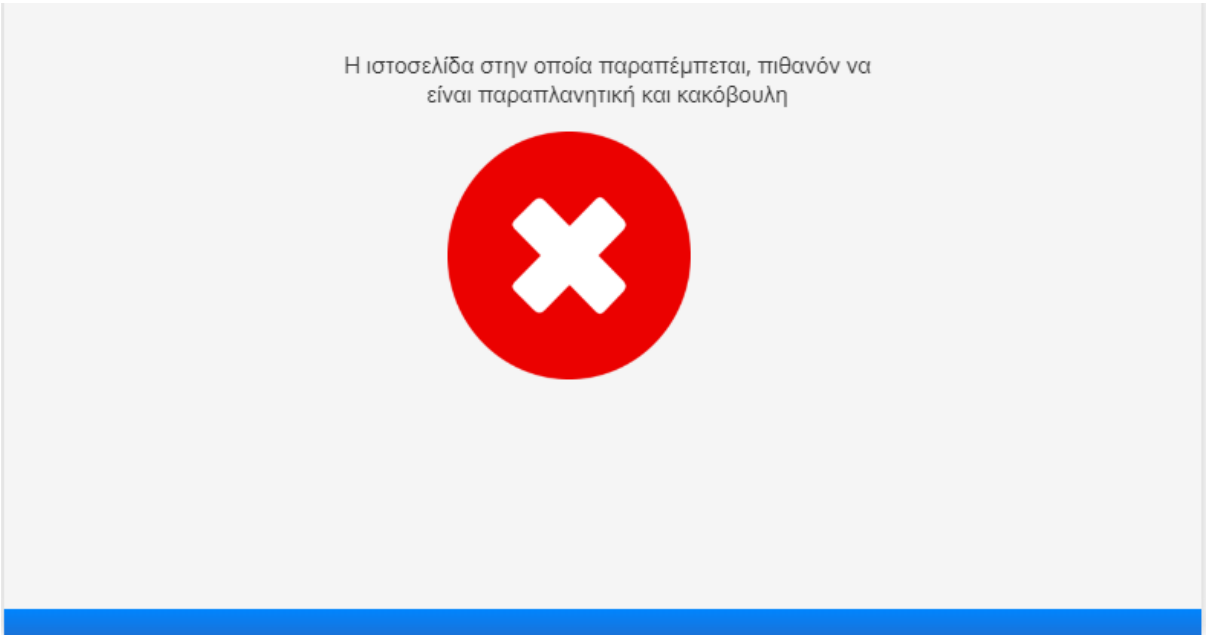
Εικόνα 5.40: Σενάριο 7 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Η ορθή απάντηση του σεναρίου, βρίσκεται στη πρώτη επιλογή όπου προτρέπετε να αγνοήσει το μήνυμα.



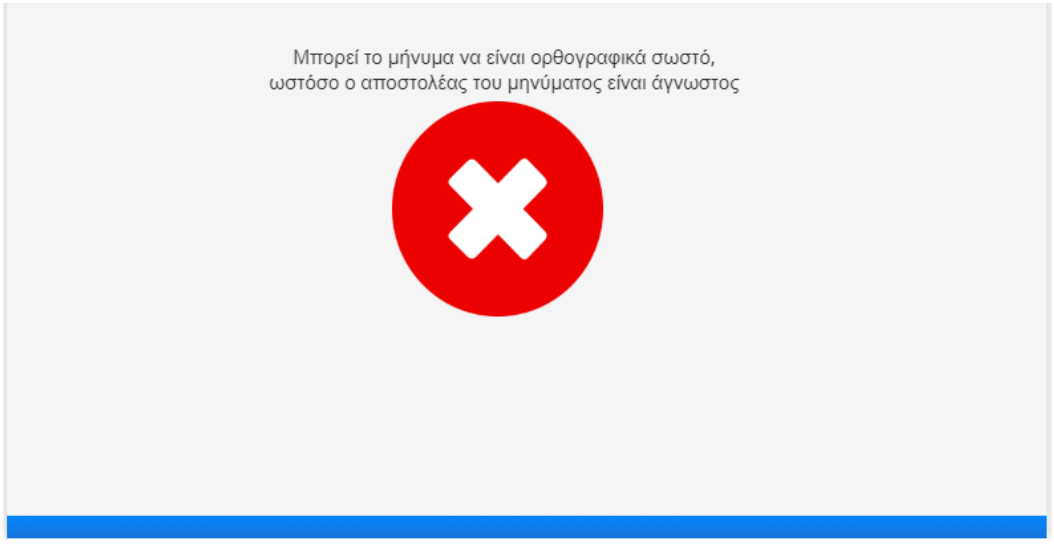
Εικόνα 5.41: Σενάριο 7 - Εικόνα Ορθής Απάντησης

Αν ο συμμετέχοντας επιλέξει τη δεύτερη επιλογή, τότε ενημερώνεται για το λάθος του, εφόσον όπως αναγράφεται και στην εικόνα που παρουσιάζεται, η ιστοσελίδα στην οποία τον παραπέμπει το μήνυμα, πιθανόν να είναι παραπλανητική και κακόβουλη.



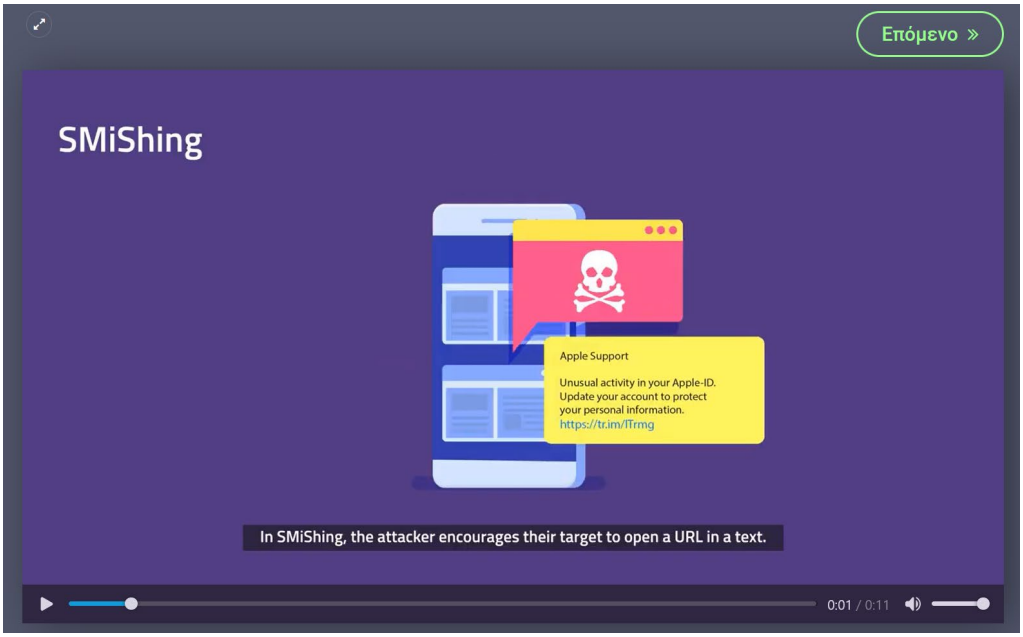
Εικόνα 5.42: Σενάριο 7 - Εικόνα Λανθασμένης Απάντησης

Λάθος αποτέλεσμα παρουσιάζεται και στην τρίτη επιλογή που έχει στη διάθεση του ο συμμετέχοντας. Αυτό προκύπτει από το γεγονός ότι ο αποστολέας του μηνύματος είναι άγνωστος



Εικόνα 5.43: Σενάριο 7 - Εικόνα Λανθασμένης Απάντησης

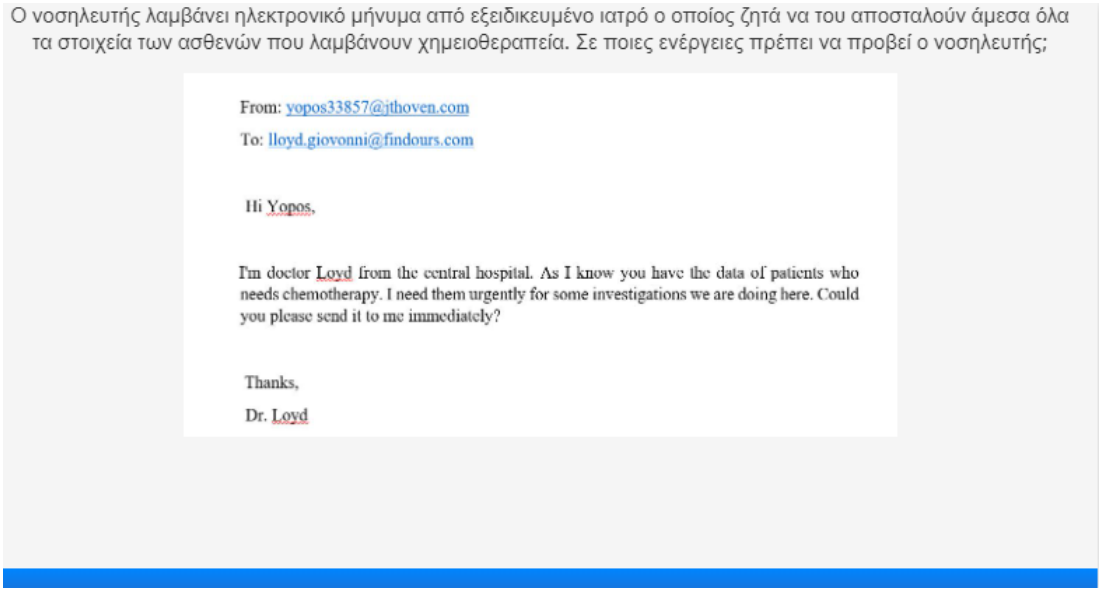
Εφόσον ο συμμετέχοντας ενημερωθεί για τη λάθος του επιλογή, προβάλλεται βίντεο μικρής διάρκειας αναφορικά με τις επιθέσεις SMSishing, μέσα από το οποίο ενημερώνεται για τις εν λόγο επιθέσεις.



Εικόνα 5.44: Σενάριο 7 – Ενημερωτικό Βίντεο

Το τελευταίο σενάριο της δραστηριότητας, αναφέρεται στις επιθέσεις BEC οι οποίες εκτελούνται με τη χρήση ηλεκτρονικού μηνύματος. Στο συγκεκριμένο σενάριο, παρουσιάζεται ο νοσηλευτής να λαμβάνει ηλεκτρονικό μήνυμα από ιατρό ο οποίος ζητά από τον νοσηλευτή να του αποστείλει άμεσα τα στοιχεία όσων ασθενών λαμβάνουν

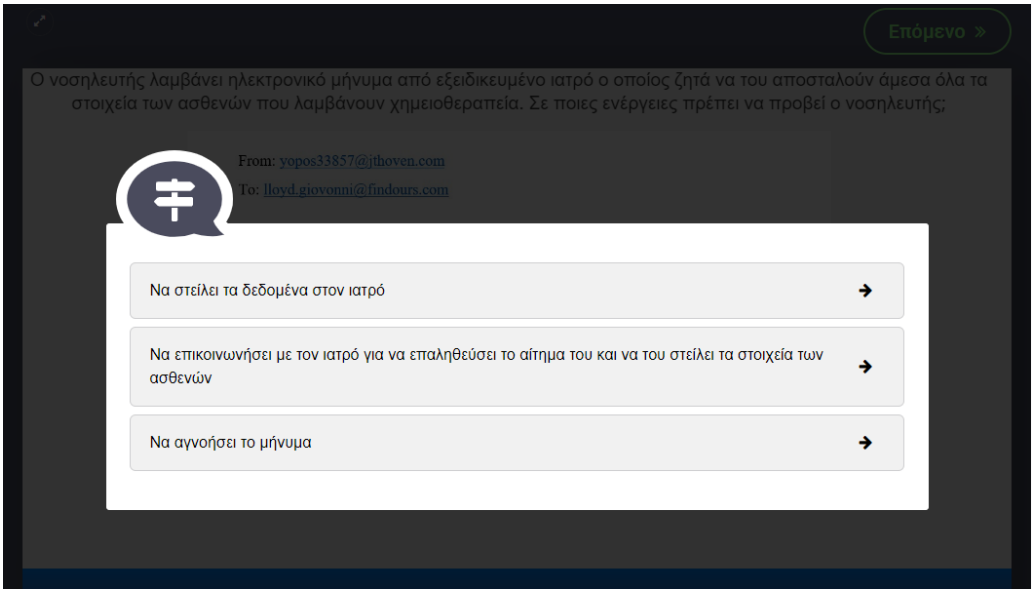
χημειοθεραπεία. Το ερώτημα που τίθεται είναι σε ποιες ενέργειες πρέπει να προβεί ο νοσηλευτής.



Εικόνα 5.45: Σενάριο 8 - Εκπαιδευτικής Δραστηριότητας

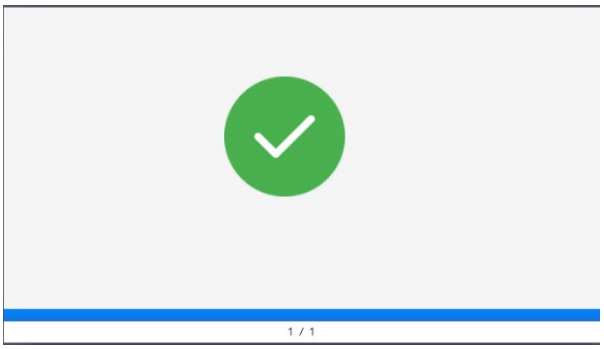
Οι επιλογές που έχει στη διάθεση του ο συμμετέχοντας είναι:

1. Να στείλει τα δεδομένα στον ιατρό
2. Να επικοινωνήσει με τον ιατρό για να επαληθεύσει το αίτημα του και να του στείλει τα στοιχεία των ασθενών
3. Να αγνοήσει το μήνυμα



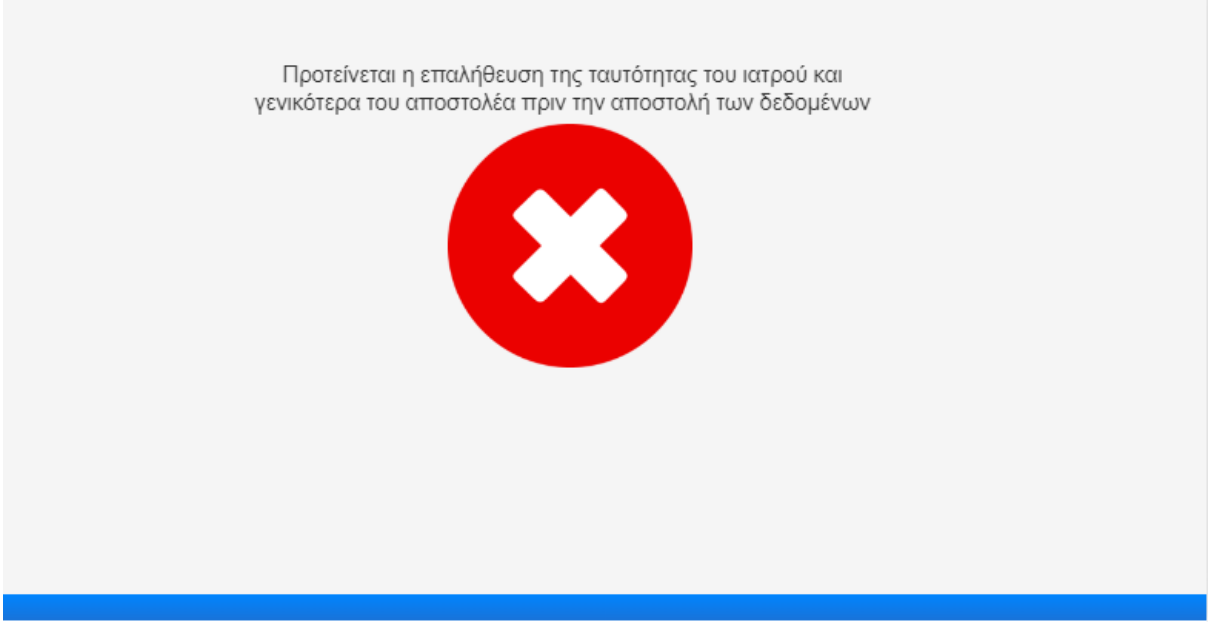
Εικόνα 5.46: Σενάριο 8 - Επιλογές Εκπαιδευτικής Δραστηριότητας

Η δεύτερη επιλογή στην οποία προτείνεται να επικοινωνήσει με τον ιατρό για να επαληθεύσει το αίτημα του και στη συνέχεια να του στείλει τα στοιχεία που ζητεί, είναι η σωστή απάντηση.



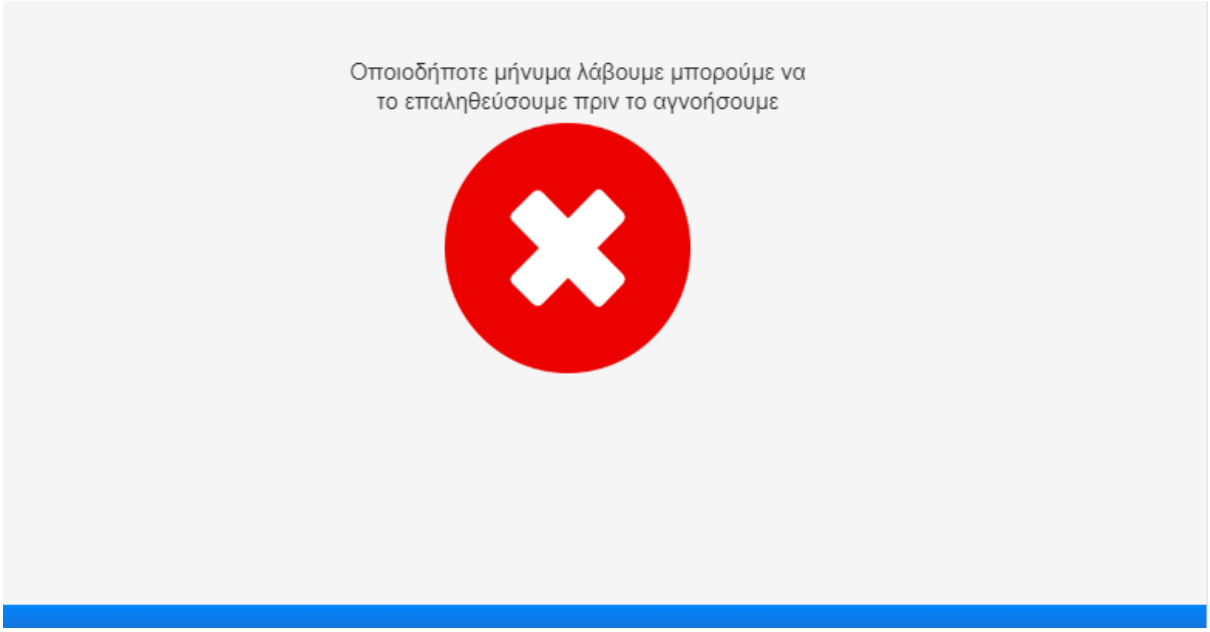
Εικόνα 5.47: Σενάριο 8 - Εικόνα Ορθής Απάντησης

Σε αντίθετη περίπτωση και επιλογή της πρώτης απάντησης, η απάντηση θεωρείται λάθος εφόσον δεν προέβη σε κάποια επαλήθευση του αποστολέα.



Εικόνα 5.48: Σενάριο 8 - Εικόνα Λανθασμένης Απάντησης

Λανθασμένη απάντηση θεωρείται και η τρίτη επιλογή, γιατί υπάρχει το ενδεχόμενο ο ιατρός όντως να χρειάζεται τα στοιχεία που ζητεί. Σε αυτή τη περίπτωση, προτείνεται η επαλήθευση του μηνύματος πριν την αγνόηση του.

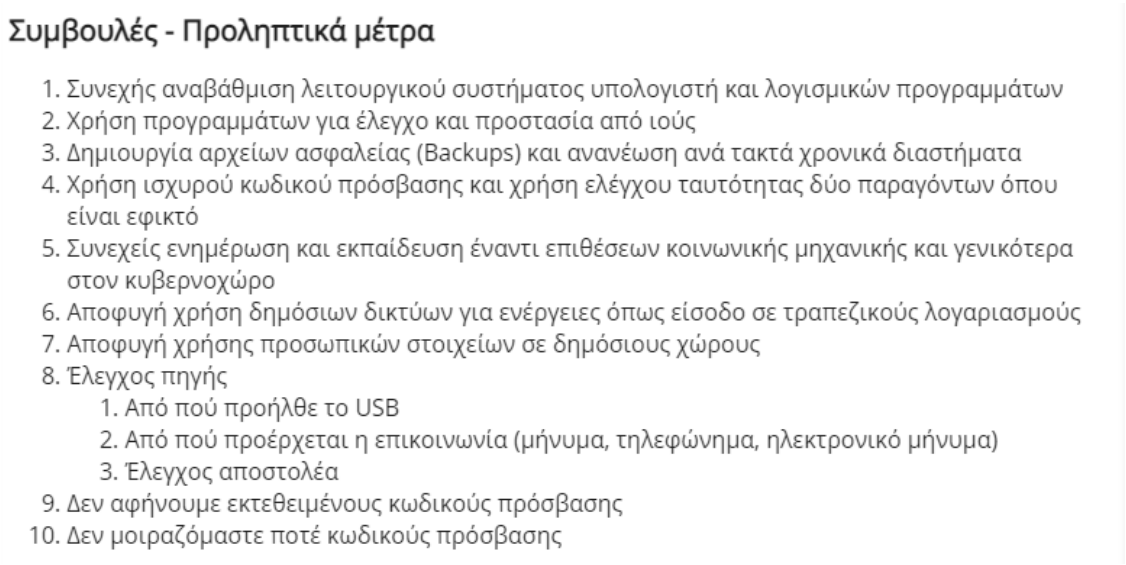


Εικόνα 5.49: Σενάριο 8 - Εικόνα Λανθασμένης Απάντησης

Στη συνέχεια προβάλλεται σχετικό βίντεο αναφορικά με τις επιθέσεις BEC.

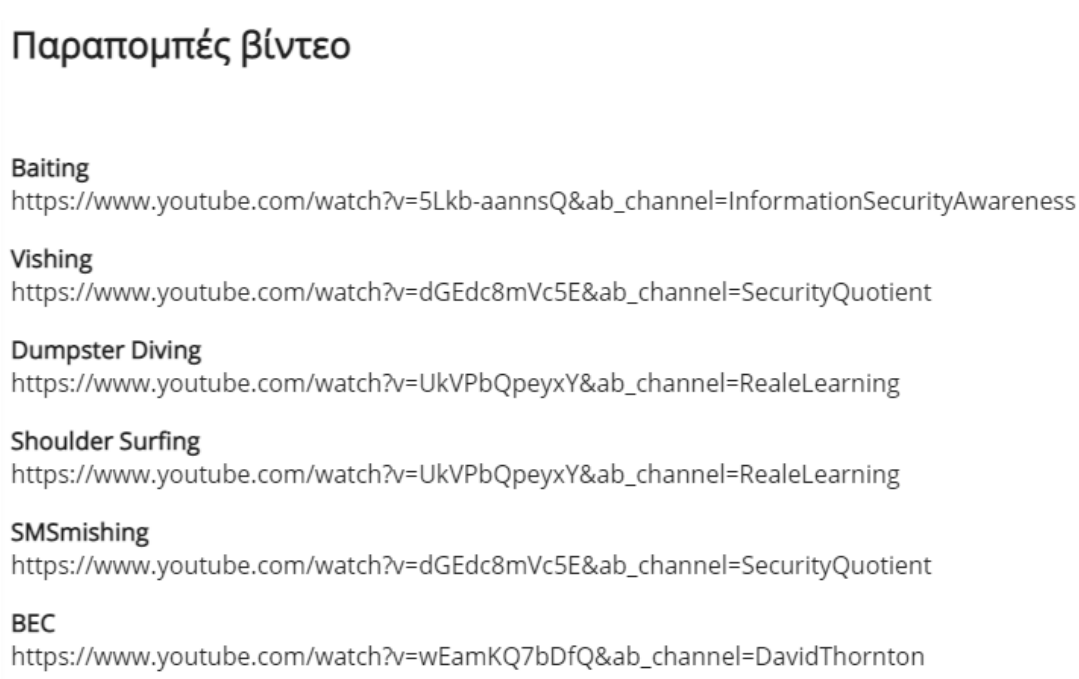
Εικόνα 5.50: Σενάριο 8 – Ενημερωτικό Βίντεο

Με το πέρας των σεναρίων, παρουσιάζεται στον χρήστη 10 γενικές συμβουλές και προληπτικά μέτρα τα οποία απεικονίζονται στην πιο κάτω εικόνα και μπορούν να αποτρέψουν επιθέσεις Κοινωνικής Μηχανικής και να προστατέψουν τον χρήστη.



Εικόνα 5.51: Συμβουλές – Προληπτικά Μέτρα

Ως τελευταία οθόνη της εκπαιδευτικής δραστηριότητας, παρουσιάζονται οι σύνδεσμοι οι οποίοι παραπέμπουν στα βίντεο που έχουν χρησιμοποιηθεί και προβληθεί κατά την δραστηριότητα. Σχετική εικόνα με τις παραπομπές είναι η ακόλουθη:



Εικόνα 5.52: Παραπομπές Βίντεο

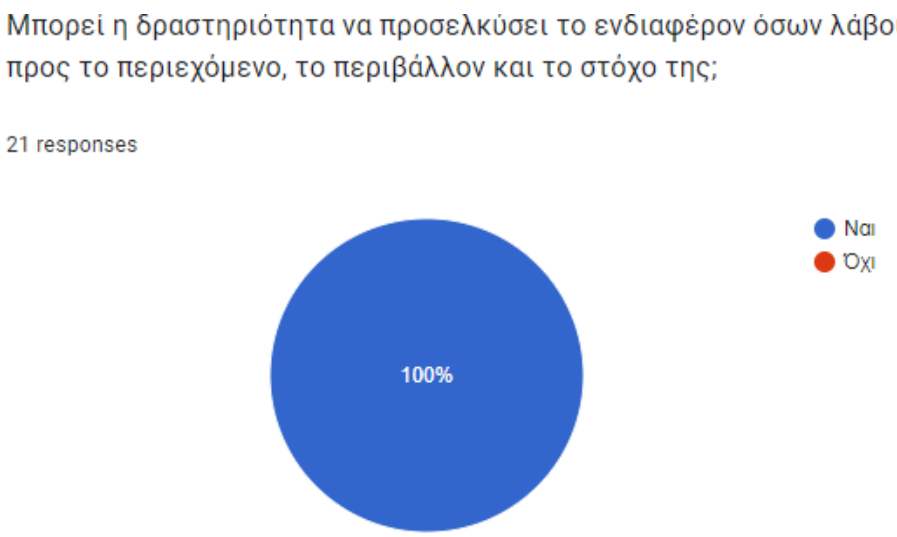
Κεφάλαιο 6

Αξιολόγηση Εκπαιδευτικής Δραστηριότητας

Στο κεφάλαιο αυτό, παρουσιάζονται τα αποτελέσματα αξιολόγησης του περιεχομένου της εκπαιδευτικής δραστηριότητας. Η αξιολόγηση πραγματοποιήθηκε σε μορφή ερωτηματολογίου έπειτα από την εκπαιδευτική δραστηριότητα και συμπληρώθηκε συνολικά από 21 άτομα τα οποία είναι γνώστες του αντικειμένου. Το ερωτηματολόγιο υλοποιήθηκε στη πλατφόρμα 'Google Forms' και αποτελείται από διάφορες ερωτήσεις, σχετικά με τον τρόπο υλοποίησης, το εύρος κάλυψης και την αποτελεσματικότητα της δραστηριότητας έναντι των επιθέσεων Κοινωνικής Μηχανικής.

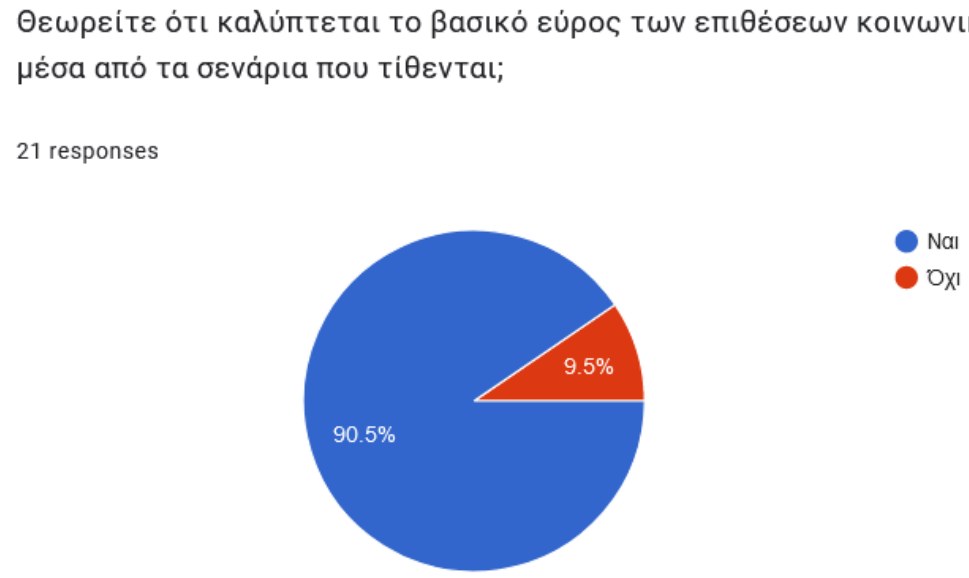
Τα αποτελέσματα του ερωτηματολογίου είναι ενθαρρυντικά, εφόσον μέσα από αυτά απορρέει το συμπέρασμα ότι η εκπαιδευτική δραστηριότητα, μπορεί να συνδράμει στην αντιμετώπιση της Κοινωνικής Μηχανικής και συνάμα στην ενημέρωση των πολιτών.

Αναλυτικότερα, από τα αποτελέσματα της αξιολόγησης, διαπιστώνεται ότι ό στόχος της δραστηριότητας επιτυγχάνεται, εφόσον όπως φαίνεται και στην ακόλουθη εικόνα και τα 21 άτομα της αξιολόγησης, συμφωνούν στο γεγονός ότι η δραστηριότητα μπορεί να προσελκύσει το ενδιαφέρον του συμμετέχοντα.



Εικόνα 6.1: Αποτελέσματα ερωτηματολογίου – Προσέλκυση ενδιαφέροντος δραστηριότητας

Παράλληλα, όπως διακρίνεται και στην ακόλουθη εικόνα, ποσοστό μεγαλύτερο της τάξεως του 90% θεωρεί ότι οι βασικές επιθέσεις Κοινωνικής Μηχανικής καλύπτονται από τα σενάρια που περιλαμβάνει η δραστηριότητα. Η δραστηριότητα περιλαμβάνει 8 σενάρια. Ο αριθμός αυτός κρίθηκε ικανοποιητικός ώστε η δραστηριότητα να μην καταστεί κουραστική στους συμμετέχοντες και παράλληλα να περιλαμβάνει τις κύριες επιθέσεις κοινωνικής μηχανικής όπως αυτές έχουν εντοπιστεί μέσα από τη βιβλιογραφική ανασκόπηση.

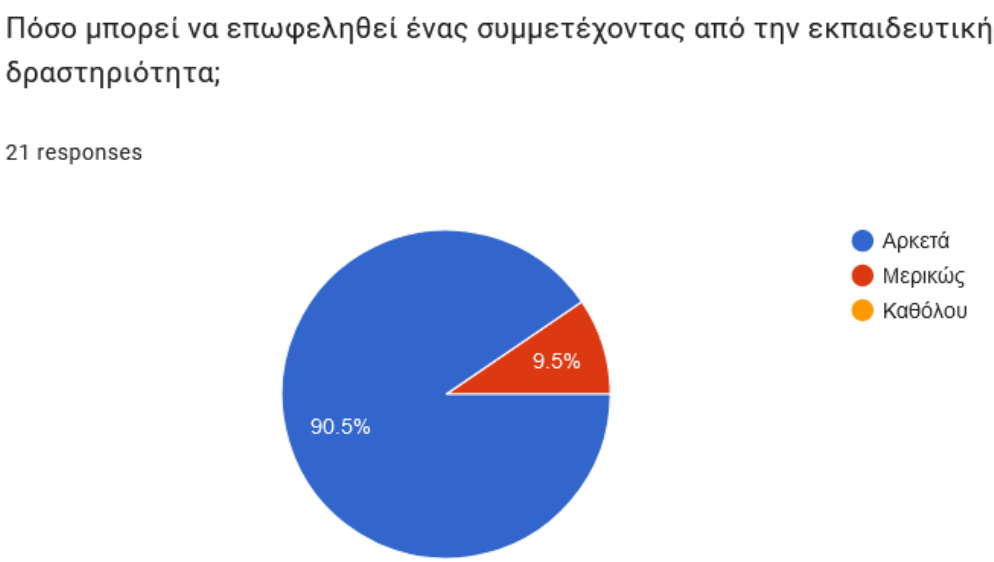


Εικόνα 6.2: Αποτελέσματα ερωτηματολογίου – Κάλυψη εύρους επιθέσεων δραστηριότητας

Σχετικά με την αποτελεσματικότητα της δραστηριότητας, ενθαρρυντικό παρουσιάζεται το γεγονός αναφορικά με το κατά πόσο ο συμμετέχοντας μπορεί να αναγνωρίσει τους τρόπους υλοποίησης μιας επίθεσης με το πέρας της δραστηριότητας. Αυτό προκύπτει από το γεγονός ότι το ποσοστό που δεν αναγνωρίζει την επίθεση είναι μηδαμινό. Αντίθετα, όπως διακρίνεται στη πιο κάτω εικόνα, ποσοστό της τάξεως του 85,7% θεωρεί ότι ο συμμετέχοντας με το πέρας της δραστηριότητας μπορεί να αναγνωρίσει την υλοποίηση μιας επίθεσης σε μεγάλο βαθμό και το υπόλοιπο 14,3% σε μερικό βαθμό.

Εικόνα 6.3: Αποτελέσματα ερωτηματολογίου – Αναγνώριση τρόπων υλοποίησης

Εξίσου ενθαρρυντικά είναι τα αποτελέσματα τα οποία παρουσιάζονται στην επόμενη εικόνα, για το κατά πόσο μπορεί να επωφεληθεί ένα άτομο από την συγκεκριμένη εκπαιδευτική δραστηριότητα. Μέσα από τις απαντήσεις, διαπιστώνεται ότι όλα τα άτομα που λαμβάνουν μέρος στη δραστηριότητα μπορούν να έχουν κάποιο ωφέλημα εφόσον το ποσοστό για καθόλου ωφέλημα είναι μηδαμινό. Αντίθετα, ένα μεγάλο ποσοστό της τάξεως του 90,5% θεωρεί ότι μπορεί να επωφεληθεί αρκετά και το υπόλοιπο 9,5% μπορεί να επωφεληθεί μερικώς.

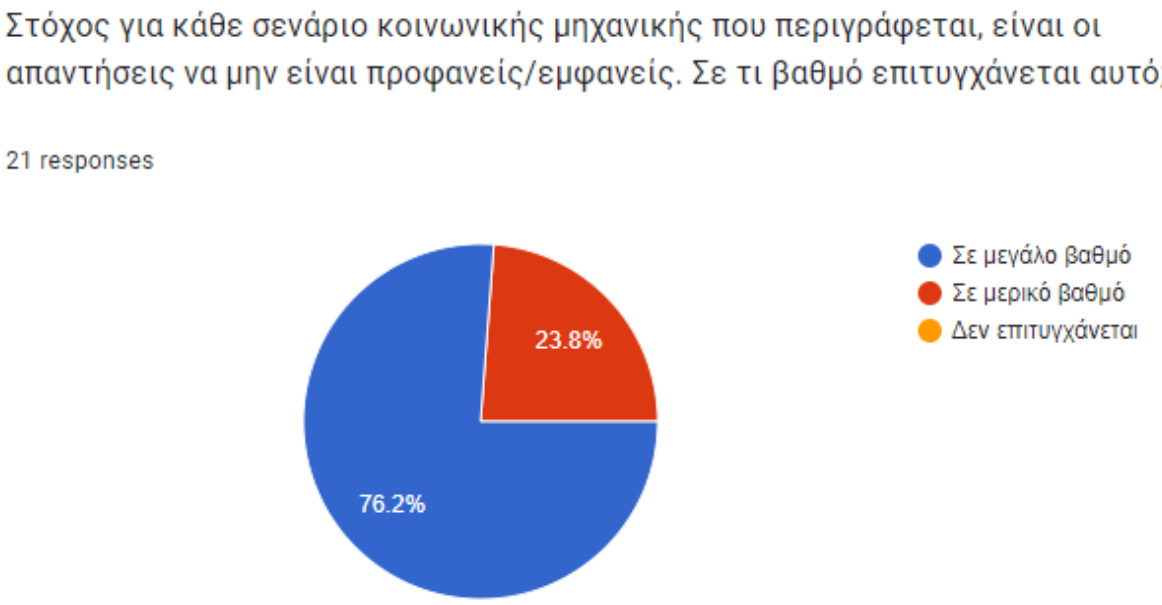


Εικόνα 6.4: Αποτελέσματα ερωτηματολογίου

Σε ερώτηση αναφορικά με τον αριθμό των σεναρίων που περιλαμβάνει η δραστηριότητα, ποσοστό 66,7% θεωρεί ότι τα 8 σενάρια είναι αρκετά, ενώ ποσοστό 23,8% θεωρεί ότι είναι ικανοποιητικά. Αντίθετη άποψη, έχει ποσοστό 9,5% που αναλογεί σε 2 άτομα και τα οποία φέρουν την άποψη ότι τα 8 σενάρια θεωρούνται λίγα για την δραστηριότητα. Τα αποτελέσματα αυτά δίνουν την εντύπωση ότι οι μέθοδοι επίθεσης Κοινωνικής Μηχανικής ποικίλουν και τα σενάρια δεν καλύπτουν όλους τους τρόπους, εντούτοις όμως ένα μεγάλο εύρος των επιθέσεων καλύπτεται πλήρως, γεγονός που καθιστά την δραστηριότητα να προσελκύει το ενδιαφέρον του συμμετέχοντα και να μην την καθιστά αδιάφορη και ανιαρή.

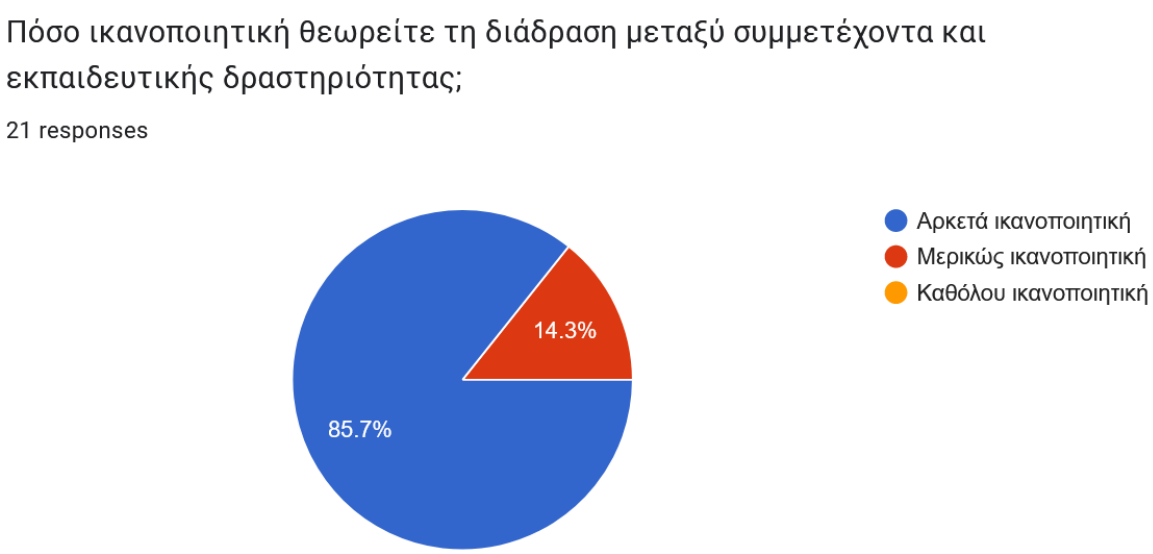
Εικόνα 6.5: Αποτελέσματα ερωτηματολογίου

Κατά την υλοποίηση της δραστηριότητας, τέθηκε ως στόχος οι απαντήσεις των σεναρίων να μην είναι προφανές, έτσι ώστε ο συμμετέχοντας να αποφασίσει για την σωστή απάντηση βάση των γνώσεων και της εμπειρίας του στο συγκεκριμένο θέμα. Σύμφωνα με τα αποτελέσματα του ερωτηματολογίου, το 76,2% των συμμετεχόντων θεωρεί ότι ο στόχος επιτυγχάνεται σε μεγάλο βαθμό και ποσοστό 23,8% ότι ο στόχος επιτυγχάνεται με μερικό βαθμό. Αυτό πιθανόν να οφείλεται στο γεγονός ότι το ερωτηματολόγιο συμπληρώθηκε από άτομα γνώστες του αντικειμένου για τους οποίους κάποιες απαντήσεις φαίνονται να είναι προφανείς. Αυτή είναι μια πτυχή που θα διερευνηθεί περισσότερο σε μελλοντική εργασία ώστε να επικαιροποιηθεί κατάλληλα το περιεχόμενο των απαντήσεων για να ελαχιστοποιήσει την πιθανότητα κάποιος συμμετέχοντας να επιλέγει προφανείς απαντήσεις.



Εικόνα 6.6: Αποτελέσματα ερωτηματολογίου

Ένας επιπλέον στόχος που τέθηκε κατά την υλοποίηση της δραστηριότητας, ήταν η διάδραση του συμμετέχοντα και της δραστηριότητας, να επιτυγχάνεται σε μεγάλο βαθμό προσελκύοντας έτσι το ενδιαφέρον του για τη συμμετοχή του σε αυτή. Όπως φαίνεται στην εικόνα που ακολουθεί, από τα αποτελέσματα του ερωτηματολογίου, παρατηρείται ότι ο στόχος επιτυγχάνεται, εφόσον ποσοστό 85,7% θεωρεί ότι η διάδραση επιτυγχάνεται σε αρκετά ικανοποιητικά επίπεδα, και ποσοστό 14,3% σε μερικώς ικανοποιητικά. Κανένας από τους συμμετέχοντες δεν θεώρησε ότι η διάδραση δεν επιτυγχάνεται.



Εικόνα 6.7: Αποτελέσματα ερωτηματολογίου

Σε ερώτημα κατά πόσο τα σενάρια και οι ενέργειες της δραστηριότητας είναι κατανοητά, κανένας από τους συμμετέχοντες δεν θεώρησε ότι τα σενάρια δεν είναι κατανοητά. Αντίθετα ποσοστό μεγαλύτερο της τάξεως του 85% θεωρούν ότι είναι πλήρως κατανοητά και το υπόλοιπο ποσοστό, θεωρεί ότι είναι μερικώς κατανοητά. Τα αποτελέσματα παρουσιάζονται στην πιο κάτω εικόνα και υποδεικνύουν ότι τα ερωτήματα και οι απαντήσεις, τίθενται σε απλή μορφή.

Εικόνα 6.8: Αποτελέσματα ερωτηματολογίου

Για τις επεξηγήσεις, που δίνονται σε περίπτωση λάθος απάντησης, ποσοστό 76,2% θεωρεί ότι όλες είναι βάσιμες και κατανοητές και ποσοστό 23,8% ότι είναι μερικές είναι βάσιμες και κατανοητές. Από τα αποτελέσματα αυτά, τα οποία παρουσιάζονται και πιο κάτω, διαπιστώνεται ότι κανένας συμμετέχοντας δεν τις θεώρησε αβάσιμες και μη κατανοητές.

Εικόνα 6.9: Αποτελέσματα ερωτηματολογίου

Με το πέρας της δραστηριότητας, επιδιώκεται ο συμμετέχοντας να μπορεί να αντιληφθεί και να αντιμετωπίσει πιθανόν επιθέσεις κοινωνικής μηχανικής. Με βάση τα αποτελέσματα σχετικού ερωτήματος, ένα υψηλό ποσοστό ίσο με 85,7% θεωρεί ότι αυτό επιτυγχάνεται σε μεγάλο βαθμό και ένα ποσοστό 14,3% ότι επιτυγχάνεται σε μερικό βαθμό. Όπως παρουσιάζεται και στη πιο κάτω εικόνα, κανένας συμμετέχοντας δεν θεωρεί ότι αυτό δεν είναι εφικτό.

Εικόνα 6.10: Αποτελέσματα ερωτηματολογίου

Η αρχική αξιολόγηση της δραστηριότητας, η οποία γίνεται από άτομα γνώστες του αντικειμένου κατέδειξε ότι ο σχεδιασμός της δραστηριότητας, και συγκεκριμένα των σεναρίων, ήταν κατάλληλη στα πλαίσια των μαθησιακών στόχων που είχαν τεθεί. Επόμενο βήμα είναι η αξιολόγηση της δραστηριότητας από μια μικρή μερίδα τελικών χρηστών έτσι ώστε να εξακριβωθεί αν χρειάζονται τροποποιήσεις πριν χρησιμοποιηθεί για την τελική εκπαίδευση των πολιτών.

Κεφάλαιο 7

Συμπεράσματα και Μελλοντική Εργασία

Η τεχνολογία στις μέρες μας ελλοχεύει διάφορους κινδύνους, αλλά παράλληλα και πολλούς τρόπους για να λάβουμε τα απαραίτητα μέτρα. Είτε βρισκόμαστε σε επιχειρησιακό περιβάλλον, είτε στο σπίτι οι κίνδυνοι ενός επεισοδίου Κοινωνικής Μηχανικής είναι μεγάλοι και η πιθανότητα να καταστούμε τα επόμενα θύματα μιας τέτοιας επίθεσης είναι ακόμα μεγαλύτερη.

Ο ανθρώπινος παράγοντας θεωρείται απαραίτητος για την προστασία έναντι των επιθέσεων Κοινωνικής Μηχανικής. Ακόμη και σε περιπτώσεις που λαμβάνονται μέτρα για την ασφάλεια και γίνεται χρήση συστημάτων προστασίας, μια λάθος κίνηση είτε οικειοθελώς είτε εξ αμελείας μπορεί να επιφέρει ανυπολόγιστες ζημιές.

Ως εκ τούτου, η ενημέρωση και εκπαίδευση έναντι των επιθέσεων μπορεί να συμβάλει σε μεγάλο βαθμό για την αντιμετώπιση τους. Αυτά τα δεδομένα προκύπτουν μέσα από την έρευνα και την υλοποίηση της εκπαιδευτικής δραστηριότητας, η οποία μπορεί να χρησιμοποιηθεί είτε από οργανισμούς, είτε ιδιωτικά για να παρέχει την ανάλογη ενημέρωση και εκπαίδευση.

Με την εξέλιξη όμως της τεχνολογίας, παράλληλα αναπτύσσονται και αναβαθμίζονται τα μέσα και οι τρόποι επιθέσεων Κοινωνικής Μηχανικής. Για το λόγω αυτό, η έρευνα, η ενημέρωση και η εκπαίδευση καθίσταται υποχρεωτικό να συμβαδίζει με τη τεχνολογία και να ανανεώνεται από τυχόν νέες μεθόδους υλοποίησης επιθέσεων.

Μελλοντική εργασία μπορεί να διεξάγεται έρευνα σε νέες μεθόδους υλοποίησης επιθέσεων Κοινωνικής Μηχανικής και στον τρόπο αντιμετώπισης τους. Παράλληλα,

μπορεί να μελετηθεί η τυχόν έξαρση ενός συγκεκριμένου τρόπου επίθεσης και ανεύρεση νέων μεθόδων για προστασία έναντι των επιθέσεων.

Επιπρόσθετα, μπορεί να ερευνηθεί κατά πόσο η συγκεκριμένη εκπαιδευτική δραστηριότητα θα προσελκύσει το ενδιαφέρον και θα έχει τα ίδια θετικά αποτελέσματα σε μικρότερες ηλικίες, εφόσον όπως αποδεικνύεται, η εφηβεία είναι η περίοδος της ζωής που κατ' εξοχήν τα παιδιά μπορούν να επηρεασθούν αρνητικά από τη χρήση της τεχνολογίας, του διαδικτύου και γενικότερα των μέσων κοινωνικής δικτύωσης.

Βιβλιογραφία

[01] C. Cordeiro and H. Barbosa, “Statistics of Cybercrime from 2016 to the First Half of 2020”.

[02] Β. Αναγνωστόπουλος, “Κοινωνική Μηχανική (Social Engineering): Τεχνικές χειραγώγησης ατόμων για την απόσπαση πληροφορίας μέσω υπολογιστικών συστημάτων,” *2021*.

[03] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey,” *Future Internet*, vol. 11, no. 4, Art. no. 4, Apr. 2019, doi: 10.3390/fi11040089.

[04] C. Hadnagy, *Social engineering: the art of human hacking*. Indianapolis, IN: Wiley, 2011.

[05] “Social Engineering Attacks and the Smart Grid | The SPARKS Project.”

[06] “17+ Sinister Social Engineering Statistics for 2022,” *WebTribunal*.

[07] “Cybersecurity.” https://www.who.int/about/cyber-security

[08] Barracuda Networks, “Spear Phishing: Top Threats and Trends.” Barracuda Networks, Jul. 2021.

[09] M. Bishop, “About Penetration Testing,” *IEEE Secur. Priv.*, vol. 5, no. 6, pp. 84–87, Nov. 2007, doi: 10.1109/MSP.2007.159.

[10] “Home - Social Engineering Academy.”

[11] embed, “Tumblr,” *Tumblr is a place to express yourself, discover yourself, and bond over the stuff you love. It’s where your interests connect you with your people.*

[12] H. Khachunts, “What is Baiting in Cybersecurity? Techniques, Examples, Protection,” *EasyDMARC*, Jul. 16, 2022.

[13] D. Aggarwal, “Network Security Attacks, Impact and Countermeasures,” vol. 6, no. 2, p. 15, 2016.

[14] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[15] K. Ivaturi and L. Janczewski, “A Taxonomy for Social Engineering attacks,”

[17] R. K. Suri, D. S. Tomar, and D. R. Sahu, “An Approach to Perceive Tabnabbing Attack,” vol. 1, no. 6, p. 5, 2012.

[18] B. Arya and K. Chandrasekaran, “A client-side anti-pharming (CSAP) approach,” in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Mar. 2016, pp. 1–6. doi: 10.1109/ICCPCT.2016.7530353.

[19] P. P. Parthy and G. Rajendran, “Identification and prevention of social engineering attacks on an enterprise,” in *2019 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2019, pp. 1–5. doi: 10.1109/CCST.2019.8888441.

[20] P. Patil and P. R. Devale, “A Literature Survey of Phishing Attack Technique,” vol. 5, no. 4, p. 3.

[21] “Protecting against spear-phishing | Elsevier Enhanced Reader.”

[22] A. Shankar and R. Shetty, “A Review on Phishing Attacks,” vol. 14, no. 9, 2019.

[23] “What are robocalls, and how can you stop them?,” *www.kaspersky.com*, Feb. 09, 2022.

[24] D. Zweighaft, “Business email compromise and executive impersonation: are financial institutions exposed?,” *J. Invest. Compliance*, vol. 18, no. 1, pp. 1–7, Jan. 2017, doi: 10.1108/JOIC-02-2017-0001.

[25] “Business Email Compromise (BEC) - The different types of attacks,”

[26] “Συνεχίζονται οι απάτες με ύποπτα μηνύματα στο Instagram-Πώς δρουν οι επιτήδειοι,” *ΡΕΠΟΡΤΕΡ*. https://www.reporter.com.cy/police/article/1010292/synechizontai-oi-apates-me-ypopta-minymata-sto-instagram-pos-droyn-oi-epitideioi

[27] “Επιτήδειοι στέλνουν mail με λογότυπα της Αστυνομίας και απειλούν με... καταγγελίες πολίτες,” *ΡΕΠΟΡΤΕΡ*. https://www.reporter.com.cy/police/article/979619/epitideioi-stelnoyn-mail-me-logtypa-tis-astynomias-kai-apeiloyn-me-katangelies-polites

[28] “The 18 CIS Controls,” *CIS*. https://www.cisecurity.org/controls/cis-controls-list/

[29] “The Social Engineer - Zefwih,” Jan. 20, 2022.

[30] M. Newbould and S. Furnell, “Playing Safe: A Prototype Game For Raising Awareness of Social Engineering,” *Proc. 7th Aust. Inf. Secur. Manag. Conf.*, vol. Perth, p. 1st to 3rd December 2009, 2009, doi: 10.4225/75/57B4004E30DE7.

[31] D. Aladawy, K. Beckers, and S. Pape, “PERSUADED: Fighting Social Engineering Attacks with a Serious Game,” in *Trust, Privacy and Security in Digital Business*, vol. 11033, S. Furnell, H. Mouratidis, and G. Pernul, Eds. Cham: Springer International Publishing, 2018, pp. 103–118. doi: 10.1007/978-3-319-98385-1_8.

[32] A.-S. T. Olanrewaju and N. H. Zakaria, “SOCIAL ENGINEERING AWARENESS GAME (SEAG): AN EMPIRICAL EVALUATION OF USING GAME TOWARDS IMPROVING INFORMATION SECURITY AWARENESS,” no. 080, 2015.